DLP REMAINS HIGH ON THE LIST OF CYBERSECURITY PRIORITIES

ATTITUDES ABOUT CLOUD SECURITY CONTINUE TO SHIFT

MOBILITY REQUIRES DILIGENCE ABOUT MALWARE

AS CYBER THREATS EVOLVE, DO FIREWALLS STILL HAVE A ROLE?

APTS: CHANGING THE SECURITY MIND-SET
Data loss prevention (DLP) has been a part of Internet security almost as long as the Internet has existed. Sometimes, though, it seems like old hat, a not very cool older uncle that is irrelevant in the face of other, sexier security solutions. But as recent high-profile events have shown, it still needs to be the focus for most organizations.

A breach at the giant retailer Target in late 2013 allowed attackers to steal millions of the company’s client credit card records. In the end, Target will pay hundreds of millions of dollars to banks to reissue credit cards, to upgrade its payment terminals, and to cover other costs. More damaging in the long run could be loss of customer confidence, something that has already cost the company’s chief executive his job.

Home Depot recently reported a similar breach, the cost of which is still unknown. Numerous less prominent breaches happen each year, and government agencies and organizations are by no means spared. Verizon, in its “2014 Data Breach Investigations Report,” ranked the public sector second on the list of industries with confirmed data losses in 2013, behind finance and ahead of retail.

The National Security Agency/Edward Snowden affair in 2013 is probably the biggest example of data loss from government, certainly since WikiLeaks. But there have been smaller though still significant breaches since then, such as an August 2014 breach of HealthCare.gov.

The reasons for government data loss are numerous, with Verizon tagging the catchall of “miscellaneous error” as the leader of all losses at 34 percent, followed by insider misuse at 24 percent and criminal malware 21 percent. Attacks and threats have become more targeted in the past few years. In its “2014 Internet Security Threat Report,” Symantec said public administration has one of the highest risks of being targeted by spear phishing, at 3 to 1.

A number of products from companies such as Symantec are supposed to protect against data loss, but an effective solution requires several things to work in combination.

The SANS Institute, which publishes a list of 20 “Critical Security Controls,” says DLP is a comprehensive approach that covers people, processes and systems that identify and protect data in use (i.e., at the endpoint), in motion across the network and at rest in storage systems.

“DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance,” the SANS report states.

In a recent survey of government organizations, SANS found that a majority had already adopted its controls as a basis for their security. Many agencies have also formally adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework, published in February 2014, which makes DLP one of its core concepts.

Two essential technologies are needed for any comprehensive DLP solution:

• Data loss or leakage products and software that help monitor, manage and protect data by classifying it and matching access to it with user authorizations. These tools can also restrict such things as copying, printing or e-mailing of the data.

• Encryption that prevents intercepted or stolen data from being read by users that aren’t authorized to have it.

A survey by the 1105 Public Sector Media Group found that agencies are also looking for other solutions to go along with DLP, including content filtering to control what content people can access, especially when delivering that content via the web, and content management that combines anti-virus, anti-spyware, anti-spam, web filtering, and information protection and control.

To be effective, respondents said, a DLP solution must...
look at all types of traffic, including e-mail, web traffic, file transfers and instant messaging. That same survey, however, pointed to the problems organizations have with deploying DLP. Only 18 percent of respondents said their organizations had already invested in DLP, while others said they were thinking of it.

But the changing information technology landscape may be forcing the issue. As agencies and other organizations push more of their data into the cloud and more uncertain environments such as the bring-your-own-device (BYOD) program proliferate, agencies will have to increasingly look to DLP as part of their underlying strategy for deploying these technologies.
The cloud, in its many forms, has been and still is a perplexing proposition for government. With its promise of enabling organizations to offload much of their IT infrastructure concerns to a managed, shared and less costly environment, it’s naturally attracted a lot of interest. But security concerns continue to dog its uptake in government.

That dynamic was visible yet again when David Bennett, chief information officer at the Defense Information Systems Agency (DISA), recently told an industry meeting in Washington, D.C., that moving some things to the cloud was very viable for agencies, but that the “crown jewels” of agency data need to stay within the defensive security perimeter.

Yet, according to the Cloud Security Alliance (CSA), cloud-related security concerns now tend to run more along the lines of general worries about security that affect all aspects of IT — data breaches, data loss, denial of service, malicious insiders — than about insecurity of the cloud itself. In a report on the threats against the cloud that people most worried about in 2013, CSA found abuse of cloud services had dropped from first in 2010 to seventh.

“This threat is more of an issue for cloud service providers than cloud consumers,” the report states, “but it does raise a number of serious implications for those providers. How will you detect people abusing your service? How will you define abuse? How will you prevent them from doing it again?”

Government solutions provider CDWG believes the persistent claim that the cloud compromises security should be laid to rest, since cloud providers now are required to use advanced best-in-class server technology and have to use internationally recognized security standards.

However, Shane Zide, a cloud client executive at CDW, said cloud users must make sure providers prove they have the necessary security for all the various flavors of cloud services they provide, including addressing their potential points of failure, which could belong to the user.

“All cloud vendors are not created equal,” Zide said, “neither is their security design and protection from internal and outside threats.”

Vendors must also answer general questions such as specifics about how they will protect agency applications in the cloud, what kind of authentication is provided, the level of encryption used for data at rest and how agency DLP policies square with what they offer.

Government organizations have gotten some help with these issues with the development of the Federal Risk and Authorization Management Program (FedRAMP), a joint government/industry effort that certifies that cloud providers meet various government security requirements. All cloud providers that federal agencies use must now be FedRAMP-certified, though agencies are still responsible for ensuring that the security for resources moved to the cloud meets government requirements.

In 2013, NIST also published a draft of its “Cloud Computing Security Reference Architecture” (SP 500-299), which sets out a risk-based framework for moving applications and services to the cloud.

The aim, said Michaela Iorga, chairman of NIST’s Cloud Computing Security Working Group, is to “demystify the process of selecting cloud-based services that best address an agency’s requirements in the most secure and efficient manner.”

However, while these NIST-driven approaches set a single set of cloud security standards across government, they are also necessarily a broad-brush approach. Agencies must go beyond them to make sure providers can meet all of their specific security requirements. Early in 2013, for example, the Defense Department dropped...
its own security accreditation process in favor of NIST’s risk-based approach, but also warned government cloud providers that they would still have to meet additional DOD needs.

Cloud security will also have to keep developing to meet future challenges, not least of which come from mobile technology, in particular BYOD. The current trend toward more targeted attacks means organizations should also expect there will be untrusted access at some point inside current security perimeters.

To grapple with these problems, and to cope with the headaches caused by such things as Infrastructure-as-a-Service, where the perimeter is constantly shifting, CSA has proposed a new standard for network security that it says would also accommodate cloud needs. Called the Software Defined Perimeter (SDP), it too incorporates NIST standards. And, at the beginning of 2014, the IT industry group SafeGov.org also proposed its own risk-based approach to cloud security.
Mobile devices in all forms are becoming ubiquitous and, for many people, they have become the primary way they access the web and communicate with others. Government’s adoption of mobile lags that of the private sector because of security concerns, but there’s little doubt that the mobile revolution is coming to the public sphere, whether government is ready for it or not.

With it will come what many people expect to be a tsunami of malware, as criminals and state-sponsored teams target government organizations and the hoards of valuable data that they possess. The only question still up for debate is when the onslaught will arrive.

A report by Kindsight Security Labs, for example, indicated a huge increase in mobile malware in 2013, with the number of mobile malware samples that Kindsight has observed up 20 times over the previous year. Actual infections increased by 20 percent, giving an estimate of more than 116 million malware-infected devices, the company said, of which 60 percent were Android smart phones.

Security vendor Symantec likewise tracked a big increase in mobile malware during the year, though it still considered the prevalence of the malware comparatively low. About 38 percent of mobile users in its survey reported having already experienced mobile cyber crime, the company said in its 2014 threat report, with lost or stolen devices being the biggest risk. Moreover, it said, the number of new malware slowed as developers worked to perfect existing malware.

“Mobile users seem to be highly susceptible to scams via mobile apps,” Symantec said, “and therefore malware need not have exploded because bad guys perhaps don’t feel they need it yet.”

However, malware will prove a major headache for government relatively soon, particularly as BYOD becomes a bigger factor.

In its “Guidelines for Managing the Security of Mobile Devices in the Enterprise” (SP 800-124) that it published in June 2013, NIST outlined a number of items for government organizations to follow:

• They should have a mobile device security policy that defines what resources can be accessed via mobile devices, and the level of access each type of device – tablets or smart phones, for instance – should have.
• They should develop systems threat models for mobile devices and the resources that are accessed through them.
• Organizations should first determine the security services needed for their environment and then acquire solutions that collectively provide these services.
• They should run pilot tests of mobile device security solutions before putting them into production.
• They should fully secure each device before letting users access it.
• They should regularly maintain mobile device security through such things as updates and patches.

However, these can give only general guidance to mobile security. They are an outline of the requirements needed to secure mobile devices and operating systems, said Mike Boyle, an NSA cryptographic expert, at an industry forum early in 2014. Organizations such as NSA then have to add things such as hardware-rooted security to the list.

Centralized resources such as mobile device, application and content management systems are also considered important for enterprise mobile security within agencies.

Because of the global popularity of Google’s Android operating system and the mobile devices that use it — they far outstrip the number of Apple iPads and iPhones — it’s a particular security focus for government agencies.
officials. The Homeland Security Department, in an August 2013 memo, pointed out that more than 40 percent of Android users were still using older versions known to have security vulnerabilities that were fixed in newer ones.

“The growing use of mobile devices by federal, state and local authorities makes it more important than ever to keep mobile OSes patched and up-to-date,” DHS said.

Help for this looks to be on its way. Samsung, which is the most popular manufacturer of Android devices, introduced its Knox (as in Fort Knox) container technology in 2013 and has been evangelizing it to private and public organizations since.

It basically isolates applications and data in specific domains on the devices, enabling each to have its own access and authentication policies. Agency IT administrators, for example, can then use Knox to allow Samsung owners to use their devices both for their personal use and for agency applications according to their level of access privileges.

“Knox was designed to bring to the market a device hardened all the way from the device itself through the operating systems and into the application layer,” said Johnny Overcast, director of government sales for Samsung Mobile. “And that allows us to check certain boxes from the compliance perspective to allow for use by both the military and public agencies.”

Knox is sparking a lot of interest in government circles, and that will probably only grow with the future launch of the next generation of Google’s operating system, Android L, which went into beta release in the middle of 2014. Although Samsung will keep machine-specific elements to itself, many other parts of Knox will reportedly be included in Android L, significantly enhancing the operating system’s inherent security and therefore boosting its appeal for government agencies.
The firewall, almost from the beginning, has been the keystone device for any organization's cybersecurity program, and in many cases it still is. However, with the evolution of threats now aimed at organizations, the traditional firewall can no longer handle the most sophisticated attacks.

But next-generation firewalls can. Or at least they provide the basis for a more complete enterprise cybersecurity plan. By including things such as application and deep packet inspection (DPI), they combine the capabilities of existing stateful firewalls with those of intrusion-detection and -prevention devices, and add capabilities such as malware filtering and Secure Sockets Layer (SSL) inspection.

The traditional firewall was not designed to look beyond IP addresses, ports and protocols, said Jeff Falcon, a senior solutions architect at CDW, which gives them a very limited ability to provide security for application classification and control. That’s a key need today, as organizations need to know who is using certain applications and the data they can access.

A widely accepted description of next-generation firewalls by Gartner Research defines a range of minimum capabilities they need to have:

- Non-disruptive, in-line configuration.
- Standard legacy firewall capabilities, such as network-address translation, stateful protocol inspection and virtual-private networking.
- Integrated signature-based intrusion prevention system engine.
- Application awareness, full stack visibility and granular control.
- Ability to incorporate intelligence from outside the firewall, such as directory-based policy, blacklists and white lists.
- Upgrade path to include future information feeds and security threats.
- SSL decryption to enable identifying undesirable encrypted applications.

With next-generation firewalls, “an organization may now begin to shift from a static ‘on-off’ switch for ports, protocols and known URLs to more of a dimmer switch strategy for safely on-boarding applications,” Falcon wrote in a recent blog post.

Most next-generation firewalls are also designed to help organizations maximize the cloud, support malware analysis and sophisticated sandboxing techniques, and enable true IPS capabilities in a single architecture, he said.

Application awareness is one of the more significant differences between next-generation firewalls and their ancestors. With that, IT administrators can get visibility into network traffic based on such things as information on actual users rather than just IP addresses, in addition to details on potential threats associated with certain applications.

Allied with DPI and intrusion detection, security can be based on patterns of activity rather than just blocking certain ports, which can obstruct necessary traffic along with that which might contain malware and other threats. Administrators can detect how certain applications behave and build knowledge of threats based on that, which is the signature of today’s more sophisticated, targeted attacks.

They can also build up information about how and when certain applications are used, giving them a better idea of when to allow the use of various non-essential applications and what they need to throttle back when the network is needed for more critical applications.

That same ability to pick and choose also allows for more careful oversight as to who has access to various functions such as networking configurations and who can set security policies or view logs, which also helps...
improve overall security.

Next-generation firewalls can, however, be even trickier to set up and manage than traditional ones because of this granularity and the complexity of the rules and policies associated with that.

Ultimately, however, there’s an even bigger question: Will firewalls be needed in the future? Firewalls are perimeter defenses and with the rise of the cloud and the development of increasingly clever security threats that easily pierce those defenses, the persistent question about if the perimeter even exists anymore is gathering steam.

Last year, in comments to armed forces media, DISA Director Lt. Gen. Ronnie Hawkins said his agency was looking at a more data-focused way of defending information rather than using a “firewall here, firewall there, firewall within a service, firewall within an organization, firewalls within DISA.”

“We’ve got to remove those and go to protecting data,” he said.

It is unlikely that firewalls will disappear completely. How next-generation technology can fit into that kind of data-centric security, however, is the question.
Advanced persistent threats (APTs) are the state of the art in terms of cyberattacks, able to penetrate the stiffest of defenses and then lie in wait for weeks or months, working away quietly to probe for an organization’s juiciest data or for the best way to damage its infrastructure, before finally striking.

Even if you’ve never heard of APTs, you likely know about them. The now infamous Stuxnet worm, which was discovered in June 2010, was launched against Iran’s nuclear power infrastructure and reportedly ruined almost 20 percent of the centrifuges it used to refine uranium. Other APTs, also with dramatic names such as Flame, Nitro, Night Dragon and Duqu, are other examples.

APTs represent the pinnacle of the current technology of attacks that target specific areas of, or people, at a company or government agency. They are very hard to detect and defend against, and their use is growing.

Between 2005 and 2013, according to NIST, cyber crimes increased nearly 800 percent, but the type shifted markedly from the brute force attacks registered at the beginning to more sophisticated, and often state-sponsored, attacks.

In 2013, NIST said, 89 percent of the callback activities detected — where malware made calls to infected servers for information, for example — was linked to APT tools made in China or by Chinese hacker groups.

An APT uses multiple phases to break into a network, avoid detection and gather valuable information over the long term, according to security firm Symantec:

- **Reconnaissance:** An attacker collects information from a variety of sources to understand the target.
- **Incursion:** Attackers break into a network using social engineering to deliver targeted malware to vulnerable systems and people.
- **Discovery:** Attackers “stay low and slow” to avoid detection, while mapping an organization’s defenses from the inside and working out how to deploy multiple, parallel “kill chains” to ensure success.
- **Capture:** They access unprotected systems and capture information over an extended period and may also install malware to acquire data or disrupt operations.
- **Exfiltration:** Captured information is sent back to the attack team’s home base for analysis and further exploitation of an organization’s systems.

How do you defend against APTs? The first thing is to acknowledge the existence of the threat in the first place. NIST, in its 2013 revision of SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” pointed out that security control baselines for government agencies do not assume that any adversaries may already have achieved a significant foothold and presence in their IT environment. That leaves them free to continue their attack on systems and infrastructure.

To more fully address APTs, it said, concepts such as insider threat protection, heterogeneity, deception, non-persistence and segmentation — all included in SP 800-53 — should be considered.

It also means changing the approach to security from building defenses that keep attackers out — the “castle and moat” approach — to assuming a more nuanced strategy. Albert Lewis, information security policy and compliance lead at Mitre, said APTs have certain characteristics: People won’t always see the initial attack, organizations can’t keep the adversary out and the APT is “not a hacker.”

He advocates a threat-based approach to tackling APTs based on understanding the threat building blocks that attackers use with APTs, sharing knowledge about threats with other organizations and taking up an agile defensive posture that can be more closely aligned with the threat.
There are no silver bullets, said Aaron Colwell, an inside solution architect specializing in network and security at CDW, and nothing will completely defend against APTs.

But organizations can take some action to try to mitigate the risks, he said, starting by securing network endpoints with DLP tools and deploying next-generation firewalls to control user access to certain websites and to analyze files and applications at the network gateway to determine if they contain malware.