Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 10, Issue 6

Protecting the Four Pillars: Physical, Data, Process and Architecture

By Jesse Cryderman

"Cyber threat is one of the most serious economic and national security challenges we face as a nation … America's economic prosperity in the 21st century will depend on cybersecurity."

—President Barack Obama, 2009

The hackers are winning.

At the end of October, Adobe Systems announced that data belonging to 38 million of its customers had been obtained by hackers, who'd infiltrated the company's systems at least two months earlier, along with the source code for three of its products. The server that housed Adobe's database also housed a PR Newswire database of customer logins and passwords, which hackers stole and leveraged for various additional exploits, such as uploading fraudulent press releases.

So much for cloud security and colocation.

Adobe's story made headlines, but its data breach isn't the biggest to date of 2013: that honor goes to Evernote and LivingSocial, both of which had 50 million customer accounts jeopardized by hackers earlier this year. Then there was the news last summer that a long-term targeted attack on systems used by Visa, 7-Eleven and even NASDAQ had exposed the credit- and debit-card numbers of at least 160 million account holders, quite possibly the largest data breach in history—so far, that is.

In 2012 hackers compromised a White House computer network; this year they merely broke into the personal email accounts of staff members and defaced the White House's website. An above-ground site (click here to see a screenshot) offers to perform accurate and detailed searches of social security numbers and phone numbers for a small fee using information it's queried from databases stolen fromthe databases of credit-card aggregators. And the vigilante hacking group Anonymous seems to be able to penetrate its adversaries' websites at will, stealing entire databases in the process.

How do they do it? And, more importantly, how can we stop it?

Unauthorized access to communications systems is becoming more sophisticated, while hackers are attacking through more avenues, and more often, than ever before. Whether you've read Verizon's "2013 Data Breach Investigations Report," HP's "2012 Cyber Security Risk Report" or one of many other sources, all signs point to an epic security fail.

Software solutions are certainly part of the story, but they only make up one leg of the table, and a security platform built on a single leg isn't sufficient to prevent the cyberattacks foisted by today's digital criminals. To fully secure communications networks, services and devices, the four pillars of security must be addressed in a dynamic fashion:

- **physical:** access to facilities and data centers;
- **data:** access, copying, reading, and manipulation rights for specific data sets;

- **process:** the ability to hijack processes;
- **architectural:** the way in which processes are structured (metadata, etc.).

Let's get physical

When I worked at an electronics factory in college, the floor supervisor had a saying: "Locks keep people honest."

Physical security is the first and foremost challenge for communications service providers (CSPs). It includes the obvious elements, like prohibiting unauthorized access to facilities with locks, key cards and biometric verification, as well as tight security protocols for physical devices such as desktop and laptop computers and storage drives. Facilities themselves need to be engineered to withstand disasters, whether natural or man-made, thus preventing interruptions in power or facilities overheating from creating attack surfaces. Physical security also extends to all network elements, including macro- and microcell sites, M2M (machine-to-machine communications) devices and even smartphones.

One of the coolest technological developments of recent years is also the cause of some of the biggest security challenges: the cloud. On-premise deployments are relatively straightforward , but what kind of visibility into physical-security parameters do cloud clients have? HP, IBM, Citrix, SafeNet, and Symantec offer cloud-security solutions that can provide the necessary visibility.

In order to offer cloud services to their customers, many CSPs, ranging from major players like Deutsche Telekom to regional mobile network operators (MNOs) like C Spire Wireless, are building their own data centers. This is no easy task, however, and CSPs often experience indecision and long construction cycles in the process. Among the solutions in the marketplace that help CSPs design their data-center operations, Netformx DesignXpert, which has received a nod from *Pipeline*, stands tall. With a catalog of more than 545,000 products and 2.45 million configuration rules, DesignXpert flourishes in a multivendor environment and enables CSPs to rapidly design and deploy safe, secure data centers that can accommodate the business needs of their customers in the most efficient way possible.

Data security

The policies that govern the ways in which data is stored, encrypted, mirrored, deleted, and manipulated have never been more important. Data security begins with encryption and redundancy: if hackers are able to break through a company's defenses and grab hold of data sets, encryption can prevent such an intrusion from becoming a major meltdown. Although total encryption has been associated with reductions in network speed, advancements in encryption solutions and processing power mean that none of a company's data should exist in a non-encrypted format.

There are dozens of disk-encryption solutions on the market with varying capabilities. Telecom-specific solutions are available from large vendors such as IBM and Cisco in addition to newer market entrants like Integra Telecom and FishNet Security. The latest generation of data-security solutions offers advanced options such as preboot authentication, two-factor authentication and hidden container support, which greatly diminish the ability of cybercriminals to gain access to sensitive data.

Mirroring data in more than one location to create redundancy is also essential. Even if certain data is useless in its encrypted form, some hackers who want to bring down services will delete or damage the supporting databases. It's extremely dangerous for data to fly solo.

How data is deleted is critical as well. Secure deletion programs like Eraser overwrite random data in empty or deleted sectors so that potentially valuable digital detritus is unrecoverable. Hard drives that are decommissioned or succumb to mechanical failure must be fully destroyed.

With the rising popularity of cloud-based solutions it's critical, from both a business standpoint and a legal one, to understand the data-security policies of any cloud providers that may be in the service chain. The same goes for third-party partners: if an app, for instance, doesn't have strong data-security policies but leverages direct-carrier billing APIs to process payments, a security hole exists.

Verizon took steps to bolster its data-encryption standards related to point-to-point transactions after discovering that "too many businesses struggle to comply with payment-card security standards, putting consumers' confidential information at risk," according to Rodolphe Simonetti, the CSP's managing director of payment-card industry services.

Process security

How do your company's systems, applications and devices react to unexpected or malformed process requests? Very often, cybercriminals are able to gain access or visibility into processes by sending requests that cause systems to fail. With the growing complexity of networks, services, applications, devices, and third-party partners, attaining end-to-end visibility of process security can be very difficult.

Fuzz testing, or fuzzing, is a valuable, automated tool that can help address this concern. As I outlined in another article in this month's issue, "What Will They Hack Next?" fuzz testing enables CSPs to expose any and all security holes related to processes that exist in their ecosystems. Fuzzing can reveal vulnerabilities in hundreds of protocols, including Bluetooth, VoIP, LTE, IMS, metro Ethernet, and XML *before* they're up and running on the network. Currently available from companies such as Codenomicon, QualiTest and P1 Security, fuzz testing is truly one of the best security solutions for next-generation service providers.

Additional processes that must be expressed as security policies are related to logging and alarms. In the event of an intrusion or even an attempted intrusion, logging leaves a trail of digital breadcrumbs that leads back to the perpetrator, while alarms should be configured to trigger a warning when processes are accessed or modified in an unexpected manner.

Architectural security

Architectural security refers to the way in which all of the security policies in an organization work together; it's only as strong as the weakest link. This is particularly true—and can be painful—in multivendor environments or, as is the case with telcos, environments that run multiple legacy systems.

Luckily, unified solutions as well as overlays exist on the market. IBM has developed an information-security architecture platform within its line of System z products that secures the entire architecture with cryptographic coprocessors and accelerators (to reduce latency associated with wholesale encryption) that are individually specialized to address various needs.

The lack of next-generation internal security policies, ones that are dynamic and reflect the latest methods used by cybercriminals, can greatly weaken architectural security. For instance, a company could have strong data, process and physical security but may not require employees to regularly update virus protections on devices used both inside and outside the office. Many hacks are perpetrated by spoofing the identities of authenticated users, so companies that haven't launched educational programs for their employees that relay the dangers of social engineering are at risk.

Securing the future

As we move into the future, CSPs must assume that everything that can be hacked will be hacked, and that there's no such thing as a small attack—just like in blackjack, a company should bet on the dealer's hidden card being a 10. The recent intrusion that exposed the data of 38 million Adobe customers was launched by a simple ColdFusion exploit many months prior to the data breach; as attacks become more and more sophisticated, this type will be the norm.

An old adage can easily be applied to the issue of cybersecurity: you can't choose how much pain you'll experience in life, but you can choose how much you'll allow yourself to suffer. By addressing all four pillars of the security platform, CSPs can prevent the pain of hacking, however unavoidable, from becoming chronic suffering.