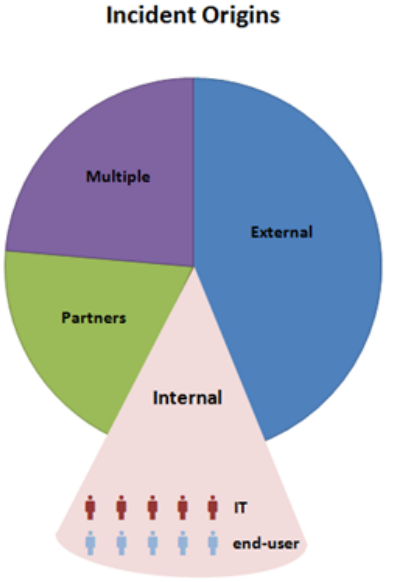
The Infrastructure 2.0–Security Connection

Lori MacVittie, 2011-22-08

#infosec #infra2 If you take one thing away from the ability to programmatically control infrastructure components take this: it's imperative to maintaining a positive security posture



SOURCE: Verizon Business 2009 Data Breach Investigations Report

You've heard it before, I'm sure. The biggest threat to organizational security is your own employees. Most of the time we associate that with end-users who may with purposeful intent to do harm carry corporate information offsite but just as frequently we cite employees who intended no harm – they simply wanted to work from home and then Murphy's Law took over, resulting in the inadvertent loss of that sensitive (and often highly regulated) data. "The 2009 CSI Computer Crime survey, probably one of the most respected reports covering insider threats, says insiders are responsible for 43 percent of malicious attacks." (The true extent of insider security threats, May 2010)

And yet one of the few respected reports concerning the "insider threat" indicates that the danger comes not just from end-users but from administrators/operators as well. Consider a very recent case carried out by a disgruntled (former) administrator and its impact on both operations and the costs to the organization, which anecdotally backup the claim "insider breaches are more costly than outsider breaches" (Interesting Insider Threat Statistics, October 2010) made by 67% of respondents to a survey on security incidents.

> The Feb. 3 attack effectively froze Shionogi's operations for a number of days, leaving company employees unable to ship product, to cut checks, or even to communicate via e-mail," the U.S. Department of Justice said in court filings. Total cost to Shionogi: $800,000.
>
> Cornish had resigned from the company in July 2010 after getting into a dispute with management, but he had been kept on as a consultant for two more months.
>
> Then, in September 2010, the drug-maker laid off Cornish and other employees, but **it did a bad job of revoking passwords to the network.** (Fired techie created virtual chaos at pharma company, August 2011)

Let us pause for a moment and reflect upon that statement: *it did a bad job of revoking passwords to the network*.

Yeah. The **network.** See, a lot of folks picked up on the piece of this story that was directly related to virtualization because Mr. Malicious leveraged a virtualization management solution to more efficiently delete, one by one, critical operational systems. But what's really important here is the abstraction of the root cause – failure to revoke access to the network – because it gets to the heart of a much deeper rooted and insidious security threat: the disconnected way in which we manage access to data center infrastructure.

INFRASTRUCTURE IDENTITY MANAGEMENT

Many years ago I spent an entire summer automating identity management from a security perspective using a variety of tools available at the time. These systems enabled IT to automate the process of both provisioning and revocation of access to just about any system in the data center – ***with the exception of the network.*** Now that wasn't a failing on the part of the systems as much as it was the lack of the means to do so. Infrastructure 2.0 and its implied programmatic interfaces were just starting to pop up here and there throughout the industry so there were very few options for including infrastructure component access in the automated processes. For the most part these comprehensive identity management systems focused on end-user account management so that wasn't as problematic as it might be today. But let's consider not only where IT is headed but where we are today with virtualization and cloud computing and how access to resources are provisioned today and how they might be provisioned tomorrow.

Are you getting the sense that we might need something akin to identity management systems to automate the processes to provision and revoke access to infrastructure components? I thought you might.

The sheer volume of "services" that might be self-service provisioned and thus require management as well as eventual revocation are overwhelming*.Couple that with the increasing concentration of "power" in several strategic points of control throughout the network from which an organization's operational posture may be compromised with relative ease and it becomes fairly clear that this is not a job for an individual but for a systematic process that is consistent and adaptable.

What needs to happen when an employee leaves the organization – regardless of the circumstances – is their access footprint needs to be wiped away. For IT this can be highly problematic because it's often the case that "shared" passwords are used to manage network components and thus all passwords must be changed at the same time. It's also important to seek and destroy those accounts that were created "just in case" as backdoors that were not specifically authorized. These "orphan" accounts, as they are often referred to in the broader identity management paradigm, must be eradicated to ensure illegitimate access is not available to rogue or disgruntled operators and administrators.

> (And let's not forget cloud computing and the challenges ***that*** introduces. Incorporating management of remote resources will become critical as organizations deploy more important applications and services in "the cloud.")

None of these processes – revocation, mass password changes, and orphan account discovery – are particularly sought after tasks. They are tedious and fraught with peril, for the potential to miss one account can be disastrous to systems. A systematic, programmatic, automated process is the best option; one that is integrated and thus able to not only manage credentials across the infrastructure but recognize those credentials that were not authorized to be created. The bonus in implementing such a system is that it, in turn, can aid in the evolution of the data center toward a more dynamic, self-service oriented set of systems.

THE INFRASTRUCTURE 2.0 CONNECTION

Thus we arrive at the means of integration with these identity management systems: infrastructure 2.0. APIs, service-enabled SDKs, service-oriented infrastructure. Whatever you prefer to call these components it is the ability to integrate and programmatically control infrastructure components from a more holistic identity management system that enables the automation of processes designed to provision, manage, and ultimately revoke access to critical infrastructure components. Without the ability to integrate these systems, it becomes necessary to rely on more traditional, old-skool methods of management involving secure shell access and remote scripts that may or may not themselves be a source of potential compromise.

The ability to manage identity and access rights to infrastructure components is critical to maintaining a positive security – and operational – posture. It's not that we don't have the means by which we can accomplish what is certainly a task of significant proportions given the currently entrenched almost laissez-faire methodology in data centers today toward access management, it's that we haven't stepped back and taken a clear picture of the ramifications of ***not*** undertaking such a gargantuan task. The existence of programmatic APIs means it is possible to incorporate into a larger automation the provisioning and revocation of credentials across the data center. What's not perhaps so simple is implementation, which may require infrastructure developers or very development-oriented operators capable of programmatically integrating existing APIs or architecting new, organizational process-specific services that can be incorporated into the data center management framework.

More difficult will be the integration of operational process automation for credential management into HR and corporate-wide systems to enable the triggering of revocation processes. For a while, at least, these may need to be manually initiated. The important piece, however, is that they are ***initiated*** in the first place. Infrastructure 2.0 makes it possible to architect and implement the systems necessary to automate infrastructure credential management, but it will take a concerted effort on the part of IT – and perhaps a highly collaborative one at that – to fully integrate ***those*** systems into the broader context of IT and, ultimately, the "business."

* This is one of the reasons I advocate a stateless infrastructure, but given the absence of mechanisms through which such an architecture could be implemented, well, it's not productive to wish for rainbows and unicorns when what you have is clouds and goats.

- Insider Threats: *Actual Attacks by Current and Former Software Engineers*
- Interesting Insider Threat Statistics
- The true extent of insider security threats
- Verizon Business 2009 Data Breach Investigation Report
- Special Report: IT Automation – Identity Management
- The Cloud Configuration Management Conundrum
- This is Why We Can't Have Nice Things
- IT as a Service: A Stateless Infrastructure Architecture Model

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com