foxtechnologies.

LINUX FOUNDATION

Managing IT Access Privileges — Not As Solved As Management Thinks

AUTHOR | DANIEL P. DERN, THE LINUX FOUNDATION

THE UNSOLVED PROBLEM

Secure, private, effective use of computers by a company (including hosted, cloud and other services as well as the company's own systems) relies on managing access privileges.

The problem isn't unique to computers. Office buildings, hotels, apartments and college dorms, for example, typically have "master keys" (or smart ID badges) that can open many-to-all of the locks in the facility, for security and other staff, while regular staff's keys or badges only work on specified rooms and entryways.

In IT, "access privilege" refers to what a given user is allowed to do in the system. A user could be a person, a job category like "admin," or a process responsible for running a problem, e.g., "www" to run an instance of the Apache web server. In Unix/Linux terminology, "root," a.k.a. "superuser," has unlimited, unrestricted privilege. (In Windows-land, this is often referred to as Domain Administrator or Local Administrator, or on individuals' systems, simply as "Admin.")

Historically, many companies have simply (but dangerously) allowed any user who needed more privilege — or claimed they did — to run as "root." Bad idea.

"Many companies think access privilege management within their IT infrastructure — providing, changing and monitoring access privileges — is a solved problem' for them, it often turns out that it wasn't," said Mark Lambiase, CTO of Fox Technologies, which sells BoKS ServerControl software — tools for managing and controlling accounts, access and privilege.

Here are Lambiase's thoughts on how companies can better control access privileges, the barriers they face in doing so, and the danger of leaving it unaddressed.

"THE RIGHT AMOUNT" OF PRIVILEGE IS ESSENTIAL, TOO MUCH IS A BAD IDEA

"Users have (or should have) well-defined and delineated access privileges, based on their job, and most likely also on their department, and current projects," says Lambiase.

Since users don't have elevated privilege "out of the box," it has to be given to them.

Elevating privilege per se within Unix/Linux systems is easy and straightforward, according to Lambiase. "Individuals can be given root privilege — wholesale unlimited power — or, using the sudo command, users (or groups of users) can be given more granular security privileges, e.g. to run specified commands with superuser or other privileges."

(If you're a Windows end user, here's a quick comparison: some programs, when you click to run them, require you to re-click (or reconfigure) to "Run As Administrator.")

The problem isn't providing elevated access privilege. The problem, according to Lambiase, is managing it — accurately,

efficiently, and cost-effectively, similarly to managing user accounts and software configurations in a cost- and time-effective way.

WHY ISN'T ACCESS PRIVILEGE BEING MANAGED EFFECTIVELY?

If access privilege is as important as Lambiase claims, why isn't it being managed effectively? (Or more effectively?)

According to Lambiase, there are a number of answers, all understandable in context — but none good enough to justify failing to have or move to solutions that meet today's requirements.

Many companies think that their access privilege management problem is a solved one, because the problem is so old, so it must have been, by now. And they have not checked lately to see whether the problem is solved inside their company, nor how well.

Some companies have started looking into the issue on their own. "Changes in compliance regimes — more requirements, larger fines for failing audits or after security breaches, etc. — led companies to look more closely and deeply at their own systems and practices," says Lambiase. "Many realized all of a sudden that they have a problem. It's really a problem that has been there all along, but they're not always noticing the historical context."

Some companies understand the problem and have been trying to solve it — but are not happy with the tools or processes that they currently have.

New and increased regulatory and compliance requirements may have outstripped existing in-place solutions, says Lambiase. New (or relatively new) regulations that require organizations to control privileged accounts include Sarbanes-Oxley (SOX), HIPAA, the Federal and North American Energy Regulations Commission (FERC/NERC), and state-level regulations such as the Massachusetts privacy law 201CMR17 and the California Information Practice Act.

Requirements for managing access privilege are "unfunded mandates." Companies see these as another cost-center item, rather than on the profit-center side, which gives IT less clout in pursuing solutions (getting budget for new software and more staff).

While the Unix/Linux 'su' ('substitute user identity') and 'sudo' ('substitute user id do') allow privilege to be changed, the commands are local to a machine or to an OS instance, with specifics defined within a configuration file. Per the next bullet, it doesn't scale well as the number of OS versions and instances skyrockets.

The number of operating system versions, images and instances, and other "IT things-to-manage" is exploding, thanks to virtual machines, containers, increasingly dense rackmount hardware, cloud-based platforms and services — and the still-growing increase in the total amount of processing and storage power being used by IT. But IT headcount to manage all this isn't growing to keep pace.

Good solutions aren't cheap. The tools to manage access privilege effectively are fairly priced, but they aren't inexpensive.

Managers have no sense of the ROI of good access privilege management. A good tool will allow IT staff to manage privilege, accounts and access more efficiently — increase their "ratios" — and be more responsive to change requests. Lambiase reports anecdotally hearing of companies who had overwhelmed IT staff using home-grown tools migrating to third-party products that, while more expensive in terms of purchase, saved IT time and money."

MANAGING PRIVILEGE ISN'T ABOUT (NOT) TRUSTING EMPLOYEES

The "I trust my employees, make everybody root" approach is simple to do and to manage -- But it's unsafe.

"Even if you can trust your employees to be honest and to not make mistakes, user credential theft by outsiders have been at the heart of many of the mega-record security breaches during the past several years," Lambiase cautions. "It's not about insider mistrust or insider threats. But when admin credentials, or

any kind of user credentials, are stolen, the outsider is — becomes — the insider."

Surely some organizations have gotten their access privileges management right?

According to Lambiase, "About ten percent of the people we talk to have their arms around this issue and think they are doing a good job — and we agree."

The rest, he — and his company — and presumably other IT consultants and solution vendors in this space — view as an educational challenge.

ABOUT FOXT

Fox Technologies, Inc. helps companies protect corporate information assets with network security and access management software as well as striving to simplify compliance and streamline administration with an award-winning access management and privileged account control solution. Our access management software centrally enforces granular access entitlements in real time across diverse server environments.

To learn more about Fox Technologies, please visit us at: **www.foxt.com**

CONTACT INFO

North America
3300 Eagle Run Drive NE, Suite 202
Grand Rapids, MI 49525
+1 877 818 3698 (Toll Free)

Sweden
FoxT Sweden AB
Kungsängsgatan 18A
SE-753 22, Uppsala
+46 18 16 00 00 (Main)

United Kingdom
400 Thames Valley Park
Reading , Berkshire RG6 1PT
+44 1189 637 681 (Main)

www.foxt.com | info@foxt.com

foxtechnologies.

You may also be interested in: Best Practices for Unix/ Linux Privileged Identity and Access Management