Why Many Companies Aren't Securing OS Permissions Adequately

AUTHOR | DANIEL P. DERN, THE LINUX FOUNDATION

When it comes to ensuring that the operating systems in your IT infrastructure are adequately secured, access-permission-wise, some companies and organizations are more up to date — secure, and compliant — than others, according to David Dingwall, architect, and business development manager, Fox Technologies (which has recently conducted an in-depth survey of over 500 IT security professionals concerning their server environment security practices).

Based on his nearly-three-decades of experience at Fox Technologies, Dingwall sees several main reasons that companies revisit — and update/upgrade — these aspects of their IT security solutions.

THE AUDITOR COMETH

"A lot of our sales are the result of auditors identifying compliance failures that must be addressed — and telling the organization they need to solve the problem, select a vendor, and show a visible project plan complete with schedule," says Dingwall. "This is probably also how our direct competitors similarly get many sales."

AGING INFRASTRUCTURES IN NEED OF A SECURITY REFRESH

Another category, according to consists of companies with very mature Unix/Linux infrastructures, whose architectural decisions were made years, even decades ago.

"Now they are depending on infrastructures behind their DMZ that are not secure," says Dingwall. "A common reason we see is that they are using very old directory services, and hasn't been an IT priority to upgrade them… but some directory services have been end-of-life'd. These are organizations that are successful, and have large infrastructures, but whose IT departments haven't been given the time and resources to address this. For example, in the survey we had done recently, about 10% of the responding organizations are still using NIS or NIS+… which have been EOL'd a few years ago."

(And this particular issue isn't recent, either — here's an Oracle blog post from 2005 about migrating from NIS/NIS+ to LDAP.)

When auditors come in with a checklist including a box for 'do you depend on any software that's been End-of-Life'd,' tick, that box gets checked. "So now these organizations now have to have a replacement program and hopefully IT now has the clout to get the resources to make this happen," says Dingwall.

That 10% outstanding NIS dependent figure came as a surprise, says Dingwall. "We didn't expect that many, because we hadn't

had the data. It's a huge market opportunity for all of us who are in this sector."

In looking for a new access privilege management tool, "Make sure the product and its vendor can integrate and replace in a straightforward way," cautions Dingwall. "Newer vendors may not know what NIS migration looks like, or integrating it may not be in their core competencies."

NEW, GROWING INFRASTRUCTURES, IPOS AND ACQUISITIONS

Another category of companies needing better OS security tools, according to Dingwall, is "the companies building brand-new infrastructures — particularly startups."

"Startups can easily go from ten to a hundred servers in their first year, and have 10,000 — probably as cloud instances — by year 3," says Dingwall. And, he adds, "People building new IT infrastructures understand databases, fulfillment, and other interfacing and API issues– but they may not understand system security well."

And even if IT isn't breached, "When they are looking at an IPO, or being acquired, in come the acquisition team," says Dingwall. "In the process of full disclosure, security holes may come up, because managing those concerns wasn't part of the original system design."

BRANCH AND REMOTE OFFICES NEED SECURITY, TOO

Companies' branch and remote offices have growing security concerns, says Dingwall. "For example, small retail branches, gas stations, retail banking, and surprisingly, mining, and distributed oil and gas operations, where each or location has one or two servers — that have to be on premises in order for operations to work — for each Point-of-Sale device and other gear to talk to. And you can guarantee somebody in the branch or local site will have to do local administration — make sure local backups happen, and make sure the link to the central site is up."

Typically, says Dingwall, "Those organizations have spent time working on the central infrastructure, but the branches have been left unchanged for the past 25-30 years. They may have changed platforms [[in the branches]] a few times over the decades, from UNIX to Windows Server to Linux. But they are still discrete machines that need their access security updated."

PERIMETER-ONLY DEFENSE ISN'T SUFFICIENT ANYMORE

"If you are only defending your IT perimeter, once an intruder penetrates inside, nothing prevents them from 'walking around inside' — gaining access to a root account, or to a sysadmin account that has approval to get to root," says Dingwall. "And many breaches aren't detected for a month or more. That's more than enough time for an intruder to download and crack entries in an encrypted password file, steal data, and more."

So, stresses Dingwall, "You need internal security as well — and to move through the network or elevate privilege on a server has to require than just a password. Ideally, use something like two-factor identification, some form of real-time identity authentication, and use least-privilege access models."

GETTING FROM "UH-OH" TO OK

The challenge, says Dingwall, is "helping the company understand the nature of the security issues in terms of privilege management, identifying what their current IT environment does and doesn't do, what today's requirements are… and that they need a plan, budget and schedule to meet today's requirements."

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