

CA Advisor

SECURITY MANAGEMENT NEWSLETTER

December 2008

Secure Both Virtual and Physical Servers With Host-Access Control Tools

By David Gormley and Nimrod Vax

You wouldn't want your bank to provide its customers with the keys to the entire branch just to open their safe deposit box, so why would you let your IT organization do the same when it comes to the company's critical physical and virtual servers?



Yet in many organizations, administrators are being given shared "root" or "administrator" access to corporate servers, exposing IT to internal security breaches, potential data loss and possible compliance violations. Disgruntled administrators are an even greater threat today than in the past, as today's server iron is more likely to be running multiple applications and several virtual servers. Compromising the host system or privileged partition on such a server would impact a far greater portion of the business than your typical departmental server.

Host-access control tools limit an administrator's ability to harm the organization (via errors or intentional activities) by doing away with the blanket assignment of root access privileges. Instead, they're assigned rights specific to the requirements of their job. IT can control who accesses a given physical or virtual server, when they can access defined resources and the precise functions they're able to perform on those resources. By consolidating access control for a broad range of platforms under a single

console, IT can become leaner, more efficient and more effective at protecting at these critical resources.

The Internal Threat

IT cannot afford to dismiss the threat posed by internal mistakes and attacks. In a white paper sponsored by CA, IDC found of 433 IT professionals in 2007, more than a third of attacks (37 percent) come from internal sources, slightly more than those that come from external sources.*

Part of the problem is that most native operating systems don't provide the ability to limit administrative privileges. It has been easier for IT to provide administrators with shared root-access for their jobs and hope that nothing goes wrong. The problem is that with root access, administrators can turn off server event logging or gain access to personnel or customer files that today would be in violation of numerous regulations.

In recent months, a 43-year old network administrator held the city of San Francisco's network hostage even as he sat in jail. The administrator gained control over the network by using administrative privileges to assign himself exclusive access. This comes on the heels of January's scandal when a trader at the French bank Societe Generale carried out a \$7.2 billion fraud in part by using administrative passwords to manipulate various systems and hide his inappropriate activities.

* IDC White Paper sponsored by CA, "Server Resource Protection: A Critical Element of IT Security," Doc # 213225, July 2008.

These individuals would not have had the same extent of privileges if their organizations had been using a comprehensive host-access control solution. Instead, they would have been assigned a very specific set of access rights for a defined period of time. Once the users changed job functions within the organization these rights could have been updated appropriately.

Nor could the administrators have used the passwords to access the servers after hours. An effective access control system would be able to restrict privileges to specific timeframes. Similarly, the access control system could also limit the employee to being able to perform specific functions on defined resources. So an administrator might be able to read, but not alter customer data during the day, for example, and never at night.

And it wouldn't matter whether the system under attack was a Windows system, a VMWare system or a mainframe. An effective access control solution provides a way to protect all of these platforms. It would restrict access across Windows, UNIX, Linux and mainframe operating systems as well as the various virtualized platforms running in the organization. CA Access Control, for example, works with over 40 operating system variants.

The time for naiveté among IT organizations has long passed. The increased use of multiple virtual servers on one physical box heightens the need for the proper segregation of duties and the application of the "least privilege" principle. In today's tough regulatory environment where lax security can expose an organization to stiff penalties, IT must find a way to facilitate productivity while protecting itself against both inadvertent errors and malicious activities that could cause significant harm. Host-access control simplifies that process.

David Gormley has over 15 years of experience in the technology industry including positions in sales, marketing, research and consulting. He is currently a member of the Identity and Access Management Marketing Team at CA. As a business consultant for Accenture and A.T. Kearney he worked on technology solutions and partnerships with Fortune 500 clients including, General Motors, AOL and Philips. Prior to that David worked at Forrester Research evaluating technology environments and consulting with partners on the adoption of emerging technologies. David graduated with a BS in Business from Skidmore College and an MBA with a concentration in Information Technology, from The University of Texas.

Nimrod Vax a member of the Product Management Team for the CA Security Management business unit and has over 9 years of experience in Software Development, including positions in R&D and Product Management. As a security specialist Nimrod designed and built cryptographic devices and access control mechanisms in various environments ranging from Windows Kernel to J2EE; and as a development manager had engaged in IAM deployments for major enterprises in North America and EMEA. Nimrod holds a BS in Computed Science from the Bar-Ilan University and an MBA with a specialization in Marketing Management from The Leon Recanati Business School in the Tel-Aviv University.

For the latest issue of CA Advisor: Security Management Newsletter, visit ca.com/newsletters/secure. To subscribe to receive future issues, or to manage your preferences, visit the [CA Preference Center](#).