

ROOT out the administrative password menace

by Nir Gertner, CTO, Cyber-Ark Software Inc.



When password management comes to mind, most managers think of their own personal passwords or the end-users' passwords used to access the network, sales database or email systems. But there is another set of passwords that is at the heart of the enterprise operation – passwords that are critical and sensitive, and yet their security and management is often overlooked.

The backbone of every enterprise infrastructure is a massive network of servers, network devices, security and other infrastructure that creates the complex communications network—or nerve center—of a company. Every day, system, network and security administrators are logging-on these critical infrastructure points for routine maintenance, repair and application of the most updated security patches. Many of them are running around with ROOT and ADMINISTRATOR privileges, either with their personal users or with commonly used accounts.

Enterprises have gone to great lengths to educate end-users and implement tools to help them choose complex passwords, avoid obvious ones, eliminate leaving them on Post-it notes, and change them frequently. It goes without saying that the same precautions apply to administrative passwords; however there are several additional security measures that need to be addressed since administrative user rights are extremely powerful, and thus call for an extra level of caution and security. To begin with, some administrative accounts must be shared among several people, for instance with network devices that support only a single defined user or when operations staff needs to solve problems after business hours. This results in administrative passwords becoming widely known and changed less frequently than required. Additionally, since administrative privileges are required for emergency and disaster recovery scenarios, only a reliable password management policy can guarantee that the correct passwords will be promptly available in these time sensitive circumstances.

Administrators have the best intentions, but the more those passwords exchange hands or remain unchanged, then the greater the likelihood of a security breach. At the same time, companies need to give near-instant access to these resources to keep the infrastructure in tip-top shape—creating a Catch-22 that often results in accessibility trumping security.

Establishing a Password Control and Change Management Program

As a stop-gap measure, many enterprises store passwords for these systems in files like spreadsheets and simple databases. A quick penetration test will show just how easy it is to get at these documents. Mismanagement of administrative passwords is a major cause for security breaches and one of the top reasons for long recovery processes from IT failures.

The problem would be easy to fix—if large organizations didn't demand near-instant access for administrators struggling to keep up with crashes and maintenance. But since this is highly unlikely to happen, organizations have to get serious and look closely at the way they save passwords and how information security and network/security management controls and manages them.

It all starts with a formal password control program that expands upon best-practice policies with technologies that enable companies to have the accessibility and security needed for administrative passwords. This type of program marries policies with controls, changes and audits to ensure best practices.

cirosec GmbH
Ferdinand-Braun-Straße 3
74074 Heilbronn
Tel.: 07131 / 59455-60
Fax: 07131 / 59455-99
www.cirosec.de

Here's a checklist of best practices that should be included as a part of an administrative password control and change management policy that can be used when creating a program and evaluating the software and services to support it.

- *Centralized Administration.* Often different IT groups control different pockets of passwords. It is important to take steps to create a centralized policy, procedures and enforcement mechanism—otherwise there is no way to ensure that each business or technical unit is doing its best to protect the keys to the kingdom.
- *Secure Storage.* Administrative passwords should be saved in a secure storage that offers strong authentication, granular access control, encryption and auditing to safeguard each and every password.
- *Worldwide, Secure Availability.* At the same time, remote access is also critical. With today's distributed enterprises, administrators need access beyond network boundaries where they can securely access and share passwords from anywhere within or outside the enterprise network.
- *A Dual-control Mechanism* that requires two or more administrators to access passwords to the most sensitive—or vulnerable—servers.
- *Routinely Change Passwords and Track History.* In addition to secure storage, the only way to ensure the long-term security of passwords is to alter them routinely.
- *Intuitive Auditing.* As passwords are used, changed or added, organizations will need to audit the whereabouts and use of passwords—without poring over log files. A new wave of regulatory compliance measures is also driving routine auditing and tracking of access to vital systems.
- *Disaster Recovery Plan.* Administrative accounts play major role in recovering from incidents that range from a simple problem to a full off-site disaster recovery. Look into technologies for automated, safe replication of vital administrative information that can guarantee the availability of those accounts in time of need.

As a final note, it's important to emphasize that the goal of the password management program is not to implement a new, overly burdensome layer of management to an already jam-packed day. With the right mix of commercially available software, best practices and a little forethought, organizations can implement these best practices quickly—without disrupting or jeopardizing critical day-to-day management functions.

About the Author

Nir Gertner has more than a decade of experience in enterprise systems security. Currently the CTO of Cyber-Ark Software, Inc., Mr. Gertner also served as software and systems engineer for BMC Software Inc. and was the chief administrator of the Security and System Department of the Central Computing Center in the Israel Defense Forces. He can be reached at nir.gertner@cyber-ark.com nir.gertner@cyber-ark.com.