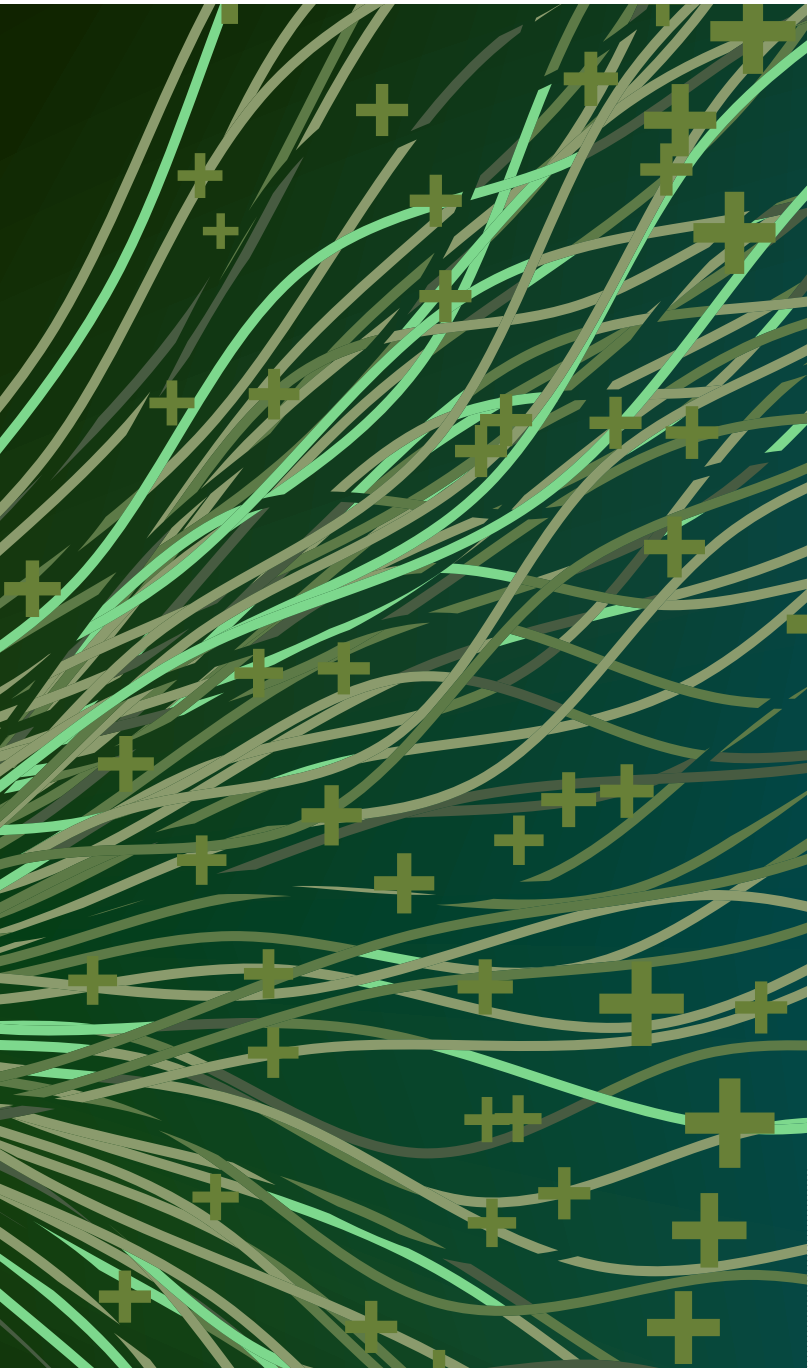

E-Guide

PREVENTING PRIVILEGE CREEP

TechTarget | SearchSecurity

PREVENTING PRIVILEGE CREEP

Mike Cobb

The security principle of least privilege is the practice of limiting permissions to the minimal level that will allow users to perform their jobs; for example, an employee working in HR doesn't need and shouldn't be granted access to the company's customer database. Enforcing least privilege plays a key role in containing the damage malicious users can cause. However, a serious mismatch between an individual's responsibilities and their privilege and access rights can occur following a change of role, department reorganization or merger. To prevent this from undermining overall security, user accounts need to be regularly audited to ensure users aren't accumulating unnecessary permissions as their roles or responsibilities change. Without a robust audit process there is a real danger of privilege creep, where a user slowly acquires new privileges without having those from former roles removed.

KEEPING PRIVILEGES ALIGNED

To prevent privilege creep and keep privileges aligned with each employee's tasks and responsibilities an organization's employee lifecycle management policy has to include a robust documented process. This process should cover the IT-related actions HR need to complete when there are changes to personnel or personnel roles, one of which has to be to notify network administrators so assigned roles and privileges can be updated and redundant accounts closed. Manually trying to manage a large number of users' privileges, though, is a time-consuming and resource-draining process and will lead to mistakes and oversights.

Investment in a privileged account security product that manages and monitors privileged users, sessions and applications will prevent the far greater costs of dealing with security incidents and data breaches caused when privileges are misassigned or abused. These products can also scale as the organization grows or moves into the cloud. Conjur's Secrets Management System, for example, can monitor, manage and audit identities and permissions across a wide range of IT infrastructures; the same is true of Centrify's Server Suite, which centralizes the creation and granting of role-based privileges across Windows, Linux and UNIX systems. Vendors such as Okta offer identity

and access management as a service tools that can make authenticating and managing users in the cloud a lot simpler and less prone to needed oversight because they integrate with existing HR systems. Enterprises who use Amazon Web Services should take advantage of its credential reporting features, which list all users in an account and the status of their various credentials, including passwords, access keys and multifactor authentication devices.

AUDITS ALWAYS REQUIRED

Even with automated role-assignment technologies, privilege creep can still occur during periods of high staff turnover, if legacy applications are upgraded or replaced, and when new applications or services are rolled out. This means account monitoring and regular audits are essential to find and correct misassigned privileges so user accounts and privileges match with HR's job descriptions. Role-based privileges should be routinely reviewed to ensure the associated privileges are still relevant and required; this should certainly be carried out after any restructuring within an organization. Remember, too, that the sensitivity of data held in different servers and databases can change over time, so access privileges will need to be realigned accordingly.

Staying on top of trusted users and their privileges is not one of IT security's most glamourous tasks but it does play a significant role in improving the security of an organization's network and cloud environments by reducing the occurrence of misassigned privileges and their misuse.

MICHAEL COBB, CISSP-ISSAP, is a renowned security author with over 20 years of experience in the IT industry. He co-authored the book IIS Security and has written numerous technical articles for leading IT publications. He has also been a Microsoft Certified Database Manager and registered consultant with the CESG Listed Advisor Scheme (CLAS). Cobb has a passion for making IT security best practices easier to understand and achievable. His website www.hairyitdog.com offers free security posters to raise employee awareness of the importance of safeguarding company and client data, and of following good practices.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.