Privilege management could cut breaches -- If it were used

http://www.cso.com.au/article/446664/privilege_management_could_cut_breaches_--_it_were_used/

January 16, 2013 14:22
By Taylor Armerding

It is well established that human error, ignorance and/or malice are more of a threat to online enterprise security than flaws in technology. An employee who falls victim to phishing or puts an infected USB drive into a workstation can let an attacker easily defeat the best security system.

But experts say technology can at least partially trump those human weaknesses. It just has to be deployed, and deployed properly.

And deployment is apparently part of the problem with "least privilege management" (LPM) -- sort of the cyber equivalent of security clearances in government. Not only do you have to be cleared at a certain level, you also have to have a "need to know" something before you are allowed access to it.

LPM basically grants privileges to applications instead of users, with the goal that only those who need access will get it. While it obviously would not entirely eliminate the risk of human error, it would reduce it.

The concept has been around for decades. J. Wolfgang Goerlich, information systems and information security manager for a Michigan-based financial services firm, said it was, "first explicitly called out as a design goal in the Multics operating system, in a paper by Jerome Saltzer in 1974."

But, it appears that so far, it has still not gone mainstream. Verizon's 2012 Data Breach Investigations Report found that, of the breaches it surveyed, 96% were not highly difficult for attackers and 97% could have been avoided through simple or intermediate controls.

LPM falls among those simple or intermediate controls Verizon noted that could save a lot of enterprises enormous grief, Goerlich said. Neither he nor other experts say it will make a system or network bulletproof, but Goerlich said, "It raises the bar by mitigating some attacks and raising the complexity of other attacks."

Bob Rudis, director of enterprise information security and risk management at Liberty Mutual, said it doesn't guarantee security -- but improves it. "It's nigh impossible to account for all types of user interaction with a system," he said. "[But] in applications that are fairly small or focused, properly implemented least privilege would be a solid and nigh unusurpable control."

Danny Lieberman, CTO of Software Associates, is a bit less confident in LPM, noting that an employee can work around LPM. "If an employee wants to access data, she can always social-engineer it out of a coworker," he said. "The main threat is not unwitting employees but malicious attackers."

The Verizon report does say that 98% of data breaches in 2011 came from external agents, but it also suggests that the success of those attacks were enabled in part by human error or ignorance. And it said: "We highly encourage organizations to run systems in a least-privilege mode."

Another problem with LPM, however, is that it is not always simple to decide who should have access to certain applications or areas.

"In an ideal world, the employee's job description, system privileges, and available applications all match," Goerlich said. "The person has the right tools and right permissions to complete a well-defined business process."

"The real world is messy. Employees often have flexible job descriptions. The applications require more privileges than the business process requires," he said. "[That means] trade-offs to ensure people can do their jobs, which invariably means elevating the privileges on the system to a point where the necessary applications function. But no further."

Mark Austin, cofounder and CTO of Avecto argued in a recent blog post that any worthwhile LPM system has to take into account both security and the user experience. "A poor user experience will inevitably lead to unhappy users and rejection of the solution, regardless of whether it makes the endpoint more secure," he wrote.

Beyond that, experts have varying views on whether putting more security trainingÃ'Â is worth the effort. Bob Rudis, who does security training seminars, describes himself as "a fairly outspoken advocate of awareness programs."

"Awareness is a strategic component of a full security program," he said. "It is not enough just to train employees and it's also not enough just to talk to them once about security awareness. It must be a continuous part of the ecosystem and culture in an organization."

Lieberman is less enthused about the effectiveness of training. "In some types of organizations, security awareness is like writing on water," he said. "The U.S. government is an example."

"If you have a dollar in your pocket I would tell you to spend it on data loss detection, not on fancy access management tools," he said.

That doesn't mean he thinks employees should be given a pass, however. "I would not waste time on security awareness training, but I would have the top management lead by example and make it clear that abuse of the company acceptable-use policy will lead to immediate termination without severance," Lieberman said.

"Like [ex Intel chairman and CEO] Andy Grove once said, 'a little fear in the workplace is not a bad thing.'"