AMAG TECHNOLOGY
A G4S COMPANY

WHITE PAPER

September 20, 2017

Bridging the Gap with Least Privileged Access

Traditionally, security directors deployed physical access control systems to secure doors. Physical security and IT security were managed independently and operated in silos. This model is no longer successful.

The security landscape has evolved and new threats have emerged. Users need to do more with their systems. Security directors must transition from controlling access to doors and buildings to managing identities. Using a policy based identity management platform, organizations can manage access via the different categories of identities (people) that enter a building. Identity access management ties systems together to manage identities (employees, contractors, vendors, visitors), rather than manage systems.

The larger the organization, the more policies and procedures it has in place. A large employee population generates a complex identity environment to manage. Employees change jobs, move from part to full time, contractor to employee or from one department to another, creating a complicated and ever changing environment for managing access.

Physical security is difficult to manage. Most companies use cumbersome manual processes that involve numerous emails and phone calls to onboard a new employee. Approvals are needed from multiple departments before granting the appropriate access, which can add days. The process is inefficient, wastes money and increases risk.

New employees, contractors and vendors need access to buildings, floors or doors, and for access to be removed when they no longer need it. Access is often not removed for terminated employees until manually caught or even worse, when there is a security breach. Large organizations often cannot keep up with manual access requests and audits due to lack of resources and poor processes. If a company cannot keep up, they fall out of compliance and risk heavy fines or sanctions against their business.

How should organizations best manage identities?

Limited Access Approach

The limited access approach grants front door and office floor access. The new employee must separately request access to all other areas he or she needs, even the access required to perform their new job. A secure option, but it requires approvals and processes immediately after the employee is hired, possibly hindering the employee because they do not have access to all areas required to do their job.

Full Access Approach

Every person hired receives full access to many areas throughout a company, either during normal working hours or 24x7. This may be effective for small businesses, such as a law firm where very few rooms need additional security, but this is the least secure option for most companies. Large organizations with facilities around the world do not need to grant a new warehouse employee in Florida access to the company's headquarter operations in Seattle.

Least Privileged Access

The least privileged access (LPA) approach provides role-based permissions to new employees to obtain access to the front door and all areas needed to perform their job. Access to additional areas must be requested by the employee. Access is granted for a predetermined amount of time and automatically deactivates access when the time limit expires. LPA provides an electronic log of all requests and an audit trail to prove compliance. LPA is the most secure and easily managed onboarding process.

LPA works well in heavily regulated industries, and is sometimes required. Organizations can match up timeframes with regulations to meet compliance. For example, background checks may last one year. Organizations can time access card expirations to match background check expiration, and help a company remain in compliance. NERC CIP regulated industries require special training to obtain access. If an employee doesn't have the training, they fall out of compliance. By syncing up LPA with NERC training, compliance is maintained.

Organizations can identify access levels per role within the company. Establishing roles in advance will create a more efficient and safe environment. Companies will save time and money, and eliminate loopholes in access.

Once set up, managing LPA is effortless. The data parameters entered into the identity management system determines who should have access and for how long. Organizations audit the parameters set up in the system to make sure they continue to meet company requirements, but that is determined by each organization.

AMAG Technology can support the Least Privileged Access approach with its Symmetry CONNECT identity management platform. For more information about Least Privileged Access, contact AMAG Technology, Vice President of Enterprise Solutions, Stuart Tucker at (310) 357-1735.

AMAG Technology
20701 Manhattan Place
Torrance, California 90501 USA
310-518-2380

Challenge House International Drive
Tewkesbury, Gloucestershire GL20 8UQ UK
+44 (0)1684 850977

21 North Avenue
Burlington, Massachusetts, 01803
800-889-9138

www.amag.com