SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Solution Snapshot

What threat protection and what value can interoperable physical and logical access control provide that strong but separate physical and logical access control cannot?

Security Executive Council Staff

Originally Published in Security InfoWatch
July 2010

Solution Snapshot:

What threat protection and what value can interoperable physical and logical access control provide that strong but separate physical and logical access control cannot?

Colby DeRodeff, Enterprise Strategist, ArcSight: If designed properly, interoperable physical and logical access control systems provide stronger authentication through location-based correlation. For example, if a user is already accessing resources in a data center in "location A," they cannot be simultaneously trying to access a geographically dispirit physical location. In this instance, the physical access could be denied pending an investigation into the situation. Either the logical account was compromised by password sharing, credential theft, etc., or the physical access system is being exploited.

This is a long-term vision, but in practice, many organizations actively use location-based correlation technology to monitor for physical and logical access violations.

By collecting both physical and logical access records, a security team can detect compromised accounts through VPN access discrepancies; or, based on correlating local resource access with the fact that a user is not physically present at the time.

To the degree that the systems can leverage and share the records of access with each other and utilize that information for authentication decisions, the more secure our enterprises will be.

William Crowell, Chairman, Senior Advisory Board to the Director of National Intelligence; member, Security Executive Council Board of Advisors: The principal gains that are achieved by converging physical and logical access controls are that you can eliminate the separate and redundant HR, Security and IT identity management systems and simplify the enrollment of personnel into the identity system. Identity is then managed cooperatively by the three organizations (or you can even combine the functions across the three into a single unit).

Operationally, there are several pluses, including the ability to combine the checking of logical identity with physical location to make sure that those accessing the IT systems are physically located inside the protected facilities, are authorized to access a particular computer in a particular area or to enforce the use of VPNs when they are remote from the facility. Using audit logs and the correlation capabilities of a SIEM together with the tracking capabilities of physical access controls, a large number of additional cross checks can be made regarding authorized and unauthorized physical and logical accesses of employees, partners and support personnel.

William M. Niemuth, Global Security & Corporate Air Transportation, Kimberly-Clark Corporation: Let's call these interoperable systems identity management. Consider the basic process of disabling the access of a user who is a threat. With an enterprise identity management system, withdrawing the person's access only needs to be done once. This can save valuable time should the person try to maliciously access the facility or its network.

The most compelling reason to implement identity management may be value. A single credential can be used for all enterprise access and seemingly fewer people are required to administer a single platform. While this appears to be an easy choice, implementing such a system, especially on a global scale, is no easy or inexpensive undertaking.

Implementing a single identity management system is security nirvana. Physical and logical security have the same loss mitigation objectives; and if identity management provides better protection at a lower overall cost, the question should not be if, but when.

Chris Wuchenich, Deputy Director of Law Enforcement and Safety, University of South Carolina: The interoperability of access control systems, both physical and logical (the status of the hardware and the systems that control the hardware) - along with the multitude of other systems found in the modern communications and control center - is becoming more essential to the efficient and effective response to an incident or other critical situation.

While responding to an incident or situation, communications center personnel are required to make timely and urgent notifications, record activities, respond to requests for information and records, and possibly activate numerous interrelated systems.

Access control systems are not the least important of these systems, and yet may well be one of the last to be activated.

An "open standard" or equivalent interoperability standard would enable communication center staff to manage multiple systems through a single interface, resulting in a more effective and immediate response to incidents and critical situations.

Next month's question: What threats should small and mid-sized businesses be considering in 2010 and beyond?

For more information about the Security Executive Council, please visit www.securityexecutivecouncil.com/?sourceCode=std. The information in this article is copyrighted by the SEC and reprinted with permission. All rights reserved.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year “retained” services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com