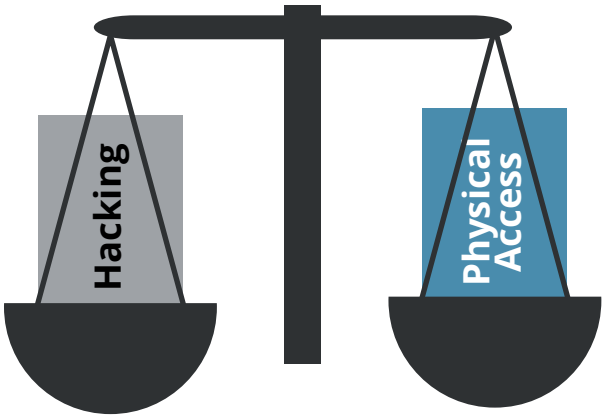
How your doors should be protecting your data and supporting GDPR compliance

Published 15 June 2016 www.securitybuyer.com

Organisations install or update their physical access controls in order to protect their most valuable assets – principally their people and their data – from external threats. However, in the virtual domain, it's not just external threats, such as hackers and viruses, which have to be protected against; the biggest unresolved information security challenge is 'insider threat'[1]– both deliberate and accidental. So organisations must also be able to protect their data from their people. Typically, access controls for the physical and virtual domains are handled separately, when in fact an integrated approach offers far greater scope to protect the people, the data and the data from the people.

Physical access controls provide people who are trying to enter through doors with a similar experience to when attempting to access IT resources in the virtual domain; they are required to submit one or more identification credentials (passcode, contactless RFID card or biometric identifier) which are validated against a database of users and their permissions before access is granted. However, the systems for managing access control in the physical and virtual domains are often very different and either not linked or only periodically synchronised.



This separation of physical and virtual access management systems creates a security risk due to the processes for staff, and contractor, on-boarding/off-boarding not being automatically joined-up across both domains. 36% of desk-based workers in the UK and US report they are aware of having continued access to a former employer's systems or data[2]. Such a gap in security is not going to meet the requirements of the new European GDPR[3] – to install solutions that "provide data protection by default."

Beyond eliminating the security gaps between separate access controls for the physical and virtual worlds, a converged solution with real-time, location-aware, decision-making can empower access controls to better address other compliance needs. For example – sensitive data like medical records[4] and customer payment card details[5] should not be accessible to IT users who are outside secure areas, where they may be copied or seen by unauthorised people.

Enhanced security and compliance aren't the only benefits of a converged approach to access control. Separate systems commonly duplicate IT resources, such as; the databases handling employee access rights, the infrastructure to provide system resilience and the network connections to respective end-points. This duplication produces an additional data maintenance overhead and a level of IT support effort compounded by the overall system complexity. A converged solution can streamline the necessary infrastructure, making it both simpler to manage and easier to set-up.

When it comes to deciding how best to go about converging physical and virtual (or 'logical') access controls, the first thing to consider is which of the two approaches may best offer an overall solution:

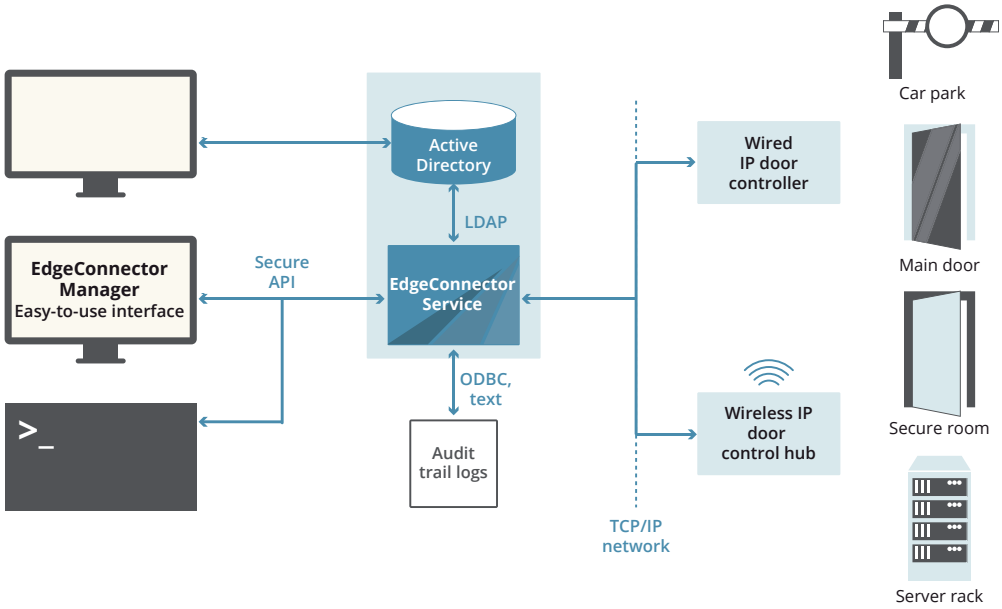
Physical access control systems normally rely on localised decision-making by controller hardware, placed near doors, which operate off-line and only receive updates of user access rights periodically from a separate database holding the personnel permissions. This architecture typically doesn't support real-time implementation of changes to access rights and is not easily scaled across multiple sites – which requires the addition of synchronisation appliances between the databases for each site.

Logical resource access is usually validated in real-time against a centralised database of users (typically Active Directory) and designed to scale across all users anywhere on the WAN. Also there are well established practises for managing permissions to IT resources through the definition of role-based profiles that can be easily assigned to individuals in the directory by HR or Security teams using identity management applications such as Sailpoint, Oracle Identity Management or Microsoft Identity Manager. This enables access rights to be assigned and managed by the appropriate team in an organisation.

Given the well-developed role-based security model of the IT domain, and real-time implementation of updates to user permissions, this approach lends itself to supporting the need for data protection by default. The scalability of centralised decision-making (whether cloud-based or hosted in-house) also makes it far easier to extend physical access controls across multiple sites.

EdgeConnector is a physical access control solution, created by IT security professionals, that delivers real-time, location-aware, dynamically converged physical and logical access decision-making. Based on Active Directory (or other existing LDAP database) – no other database is required. Use existing ID management applications, or EdgeConnector's own management tools and APIs, to provision role-based physical access rights. Leverage IP network infrastructure and resilience to easily extend physical access controls from server racks to secure rooms and multiple sites world-wide.

EdgeConnector access control solution architecture



When you've seen EdgeConnector – you'll be asking why all physical access management systems aren't designed the same way.

Enhanced security | Simple management | Easy installation

EDGECONNECTOR

www.edgeconnector.com

References:

[1] Infosecurity Europe 2015 attendee feedback: 42% indicated insider threat as being the biggest unresolved information security challenge

[2] Infosecurity-magazine.com July, 2014

[3] GDPR (General Data Protection Regulation) – New, harmonised, EU Data Protection & Privacy Law: Coming into force in May 2018, replacing European Data Protection Directive 95/46/EC. As a regulation the GDPR will be directly applicable to all EU member states without need for national legislation. It requires prompt compulsory notification of breaches and imposes large financial penalties for non-compliance.

[4] HIPAA – Health Insurance Portability and Accountability Act

[5] PCI-DSS – Payment Card Industry Data Security Standard

© 2016 Dot Origin Ltd. - All rights reserved