杜绝服务器攻击的五大基本考量因素

全球商业在 2020 年经历了一次彻头彻尾的变革，许多人不得不在仓促间向远程分散的计算快速转变。在网络安全领域，这类情况却是网络攻击者的良机。

毫不意外，根据 IBM 安全部门发布的年度报告——2021 IBM X-Force Threat Intelligence Index（2021 IBM X-Force 威胁情报索引），2020 年，勒索软件、网络钓鱼和恶意软件攻击总体上升，此外，访问服务器成为第三大最普遍的攻击类型。该报告将服务器攻击定义为“威胁行为人利用所盗取的服务器信用证、安全隐患或其他方式，获得对受害者服务器未经授权的访问权”。

实际上，在数据已然成为全世界最具价值资产的情况下，数据的隐私和道德合规管理必须是各组织和数据中心的重中之重，在远程工作日渐成为常态非例外的时代，尤其如此。

智能电力管理解决方案和信息及通信技术 (ICT) 基础设施专家 Chatsworth Products (CPI) 建议数据中心采用稳健的访问控制系统措施，做为其综合网络安全框架的一部分。

尽管数据隐私标准和法规要求为数据处理和存储设备提供物理访问控制措施，但具体的技术方法则是各组织自行决定的。

整体合规性要求一种方法满足：

物理安全数据处理和存储设备

识别和管理经授权的访问者

管理对物理安全空间的访问

记录对物理安全空间的访问

搭建访问控制系统时的五大基本考量因素

物理安全第一道防线

对于企业拥有的单租户场所，房间级安全就以足够。尤其是在多租户数据中心 (MTDCs)，又称作共用场地设施和远程场所，机柜级别的物理访问控制能简化管理并防止未经授权的用户访问存有数据的服务器和交换机。

电子锁和访问控制系统将监控、归档和访问控制自动化，并能在访问权限改变或信用证丢失或被盗的情况下实现快速重新编程。

钥匙和权限管理

当使用钥匙锁保证设备机柜安全时，公司必须拥有强大高效的钥匙管理程序。无论机柜如何配置钥匙，
都需要一个强大的系统用于访问归档。

相比之下，电子门禁则能用新访问码快速重新编程，且无需修改硬件。每个用户均有不同权限，且软件中的权限设置自动归档所指派的访问码（密匙）。

记录报告和审核

让用户在从建筑物正门访问时登录，能确保将该人员进入建筑物的记录归档，但其对单个机柜则的访问记录则无法归档。

电子门禁和访问控制系统将对机柜级别的访问记录自动化并启用用户或机柜自动报告。这能加快审核准备并有助于缩小事件调查范围。

事件反应

当发生数据泄漏时，即时事件反应至关重要。在钥匙锁系统中，IT 团队必须手动检查门和锁的状况。如果钥匙丢失或被盗，则必须给锁重新配钥匙。

电子门禁和访问控制系统简化缩短这些反应，并在某些情况下将这些反应自动化。此外，这些系统能让 IT 团队通过软件界面远程管理访问尝试和门的状态。

管辖权：IT 还是设施管理部门？

在大多数数据中心设施中，安全通过建筑物管理系统平台来部署，由设施管理部门拥有和管理。就数据中心机柜和系统而言，最多数情况下，通常由 IT 控制安全，监督数据保护和设备安全。

上述这些考量因素和能力无疑是一个明智的起点，但还有其他重要因素，二者相结合，就能创造一个完全不会过时的智能机柜生态系统。请观看 chatsworth.com/data-centers 中的视频以了解更多信息。

CHATSWORTH PRODUCTS