Data Center Security
数 据 中 心 安 全 性

主要风险
和
解决方案

地衣除尘.微信公众号　地衣除尘.微信企业号

www.cd-estt.com

地衣除尘，除尘先锋

T:+86-028-85434834/85433824-8012
Mobile:13808234900(刘小姐)

QQ:2014278941
http://www.cd-estt.com

Data Center Security Solutions

概述

您是否熟悉威胁数据中心的主要安全风险？本文概述了数据中心安全团队最常见和最重大的风险。为了帮助您解决这些风险，我们将介绍当今市场上最有效的解决方案，并说明如何在数据中心中实现日常运营。

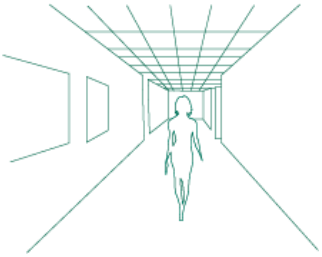
数据中心的任何风险都可能对任何业务产生重大影响。据美国联邦通信委员会（FCC）估计，大型数据中心设备的停机成本大于每小时200万美元。

今天市场上的许多安全解决方案不仅可以处理这些风险，还可以帮助企业显着提高安全和业务运营的效率。

主要风险如下：

1. 服务器故障
2. 未经检测的烟雾可能导致事故
3. 对现场个人行为的有效监控
4. 危及高层管理人员
5. 紧急情况下员工通知系统无效
6. 数据中心密钥管理效率低下
7. 由于微环境条件，设备在各个机柜中的故障
8. 网络连接失败
9. 外部黑客
10. 库存管理程序无效

请继续阅读，了解有关最新解决方案的更多信息，以帮助您确保数据中心的安全！



Data Center Security Solutions

风险1：

安全服务器故障

W当数据中心服务器发生故障时，会导致日常安全操作的重大中断。安全人员无法管理卡访问，更改授权级别或验证持卡人身份，并且不能使用任何基于Web的应用程序。访问控制门和摄像机在服务器故障期间可能会丢失与系统的连接。

如果服务器停留时间太长，现场系统控制器的事件数据无法及时上传，可能会导致重大数据丢失。

解决方案:

“ CLUSTER”软件安装多个服务器

“”集群”软件允许多个服务器通过在另一个服务器上镜像数据来相互协调工作。以这种方式，数据受到保护，并在一个服务器发生故障的情况下立即恢复。

该解决方案可帮助安全团队减轻自然灾害或人为灾难造成的损失。集群软件还允许通过在服务器之间无缝切换进行连续操作，这允许安全团队在执行服务器维护时最大限度地减少系统停机时间。

Data Center Security Solutions

风险2:

不受保护的烟雾

数据中心的火灾事故常常是电力设备的电力浪涌引起的。在火灾事件的早期阶段，所产生的烟雾可能会被嗅觉检测出来，但通常太细，而且数量太少，不能被标准的烟雾报警器，更不用说人眼检测到。

通过空调系统的循环也可能导致室内烟雾变得更加分散，这进一步降低了烟雾探测器的有效性。在火灾事件至关重要的时刻激活消防安全系统，操作中断和设备损坏往往是不可避免的。

解决方案:

非常早期的烟雾检测系统

“非常早的烟雾探测系统”或抽吸式烟雾探测器（ASD）系统通过安装一个遵循烟气将由空调系统携带的路径的“采样管”，在早期阶段检测设施中的烟雾。

该管道上的毛细管捕获空气样品并将其运送到中央测试室。在这个室内，灰尘和其他大颗粒被从空气中过滤出来，空气中的烟雾颗粒水平使用复杂的激光检测机构进行测试。然后将该数据传送到通知系统，当系统烟雾粒子水平指示即将发生的火灾事件时，该通知系统将提醒用户。

因此，ASP系统能够在几秒钟内检测到烟雾，从而使终端用户能够更容易地防止火灾和对设备的相关损害。更重要的是，与传统的烟雾探测器不同，ASP系统还具有自我监测功能，允许系统通知用户是否不能执行烟雾探测操作。

Data Center Security Solutions

风险 3:

中心区的个人无效监测数据

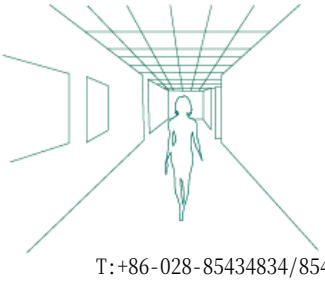
数据中心中的一个计算机室通常覆盖相当大的区域，大部分装置彼此排列。这些装置中的每一个都是由单独的人员来管理的。因此，一旦人员进入该地区，就难以进行详细的跟踪和管理。

解决方案:

实时定位系统

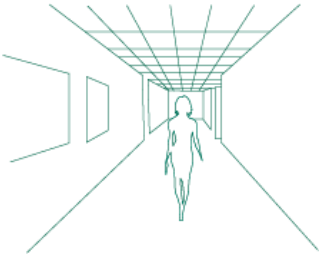
使用实时定位系统（RTLS），每个员工都需要携带无线位置标记设备。 Sentry设备安装在数据中心的主要入口路径和计算机室内。当员工进入敏感区域时，标记将识别数据发送到电子监控站，使位置跟踪软件记录员工的身份证号码以及进入敏感区域的时间。

此外，实时定位系统能够与视频监控系统和门禁系统进行接口。这允许安全人员通过收集和整合来自所有三个系统的数据，以更高的效率监视数据中心内的所有活动。



RTLTS系统具有以下功能:

- 有效和持续地监测每个员工的位置;员工进入限制区域时的通知
- 单独位置的安全人员可以通过跟踪和监控所有进入和退出数据中心的员工进行远程现场管理。
- 各种检查机制和监控员工活动的方法，包括员工实时位置，按区域的员工数据，按名称，职位，性别和其他关键搜索字词记录检查，并根据设定的时间记录检查。
- 使用虚拟站点地图监视员工运动轨迹
- 与视频监控系统的接口功能，允许员工随时检索被跟踪人员的视觉图像
- 具有开关，缩放和漫游功能的3D电子地图
- 基于角色的授权管理机制，根据他们的层次向不同的员工显示不同的信息。



Data Center Security Solutions

风险 4:

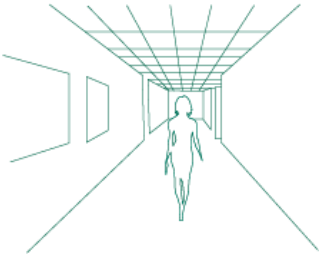
高层次的侵害管理人员

如果数据中心的授权级别高的人员受到威胁，就可能使数据中心的所有资产的安全受到威胁。数据中心最重要的安全目标之一是监控高层人员的安全，并在安全受损时立即作出回应。

解决方案:

紧急报警系统

配有紧急报警系统，高层管理人员配备无线应急报警装置，发出紧急报警信号，通知保安人员采取必要措施。



风险5:

无效警报通知程序在安全期间 事故征兆

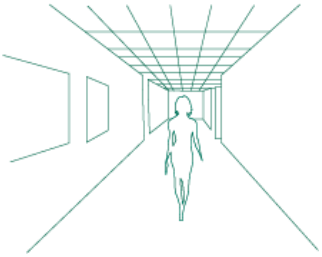
在紧急情况下，通常有必要根据其角色，位置或风险级别向不同的个人发出各种警告。在这些情况下，使用最快，最有效的方法将相关信息提供给目标群体至关重要。如果这个工作留给个别员工，错误的范围就很难避免资产甚至生命的损失。

解决方案:

质量通报系统

大众通知系统（也称为人身安全系统）是通知和保护个人的有效途径。

在安全事件发生的情况下，大众通知系统可以通过音频或视频信息，短信或电子邮件向办公楼的住户或建筑物内的特定区域发送实时信息，以鼓励所有受影响的人员进行正确的事件响应。



T:+86-028-85434834/85433824-8012
Mobile:13808234900(刘小姐)

QQ:2014278941
http://www.cd-estt.com

Data Center Security Solutions

风险6:

数据中心钥匙损失

数据中心门和锁控机器的数量需要大量的钥匙。如果这些密钥的管理是由个体员工进行的，那么系统而有效地进行这些密钥是很困难的。即使有专业人员，也难以跟踪哪些人被授权使用什么密钥，或者每个密钥的预期用途。更重要的是，在许多数据中心，使用笔和纸保存记录仍然是典型的，这使得安全人员难以保持清晰的记录。在安全事件发生的情况下，有必要逐行删除这些记录，这是高效率的使用时间。使用纸质记录，管理人员也难以实时监控关键用途和下落。在这种情况下，由于人为错误容易丢失钥匙。

SOLUTION:

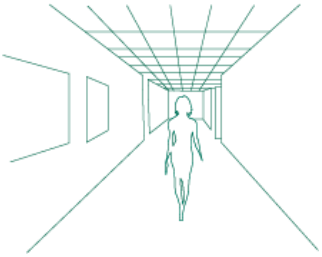
密匙管理系统

使用密钥管理系统，数据中心密钥存储在专用密钥柜中，可防止入侵攻击。使用键盘，刷卡或生物识别扫描仪自动获得键的访问，无需专业人员。系统还保存所有检索到的密钥的详细记录（包括使用的时间和日期，密钥号码，用户照片等）

该系统还包括一个完整的安全警报机制，在发生故障，操作不正确，违反授权或强制违规时立即向相关人员或部门发送警报通知。

该系统完全消除了由于人为错误或管理有缺陷而导致的丢失风险，并允许管理人员通过每个密钥上的RFID标签实时跟踪关键位置和使用情况。密钥使用授权也可以随时由安全小组进行调整。在安全事件发生的情况下，系统可以在事件发生时生成关键用途的高度详细准确的报告，并大大减少安全调查的范围。

最重要的是，将密钥管理系统与访问控制系统集成可以防止个人使用密钥和非法拷贝。



风险7:

机柜微环境检测

在数据中心计算机机房中，设备故障常常是由于个别机器周围物理微环境的条件，如次优温度，湿度等因素。

传统的环境监测系统往往侧重于整个房间，无法检测导致单件设备故障的环境条件。

解决方案:

机柜监控系统

机柜监控系统可以在各个机柜周围的环境中对温度，湿度水平，电压，电流和电源运行状态进行实时测试。这些系统还具有监测烟雾浓度，柜门状态，附近侵入者等的传感器。

如果条件低于最佳水平，则提前向相关人员发送警报通知，以帮助他们适当调整环境，防止任何潜在的损害或损失。使用单个IP地址，计算机机柜还由访问监控系统，现场LCD控制系统，视频图像捕获系统和防盗报警系统的网络支持。

所有这一切确保了在最安全的环境中，计算机房中的关键设备可以在最佳条件下连续运行。

风险8:

网络连接故障

研究表明，数据中心系统停机时间的80%发生在系统网络的修改过程中。而且，如果发生故障，90%的恢复过程用于诊断，其余10%用于恢复操作。

信息安全在很大程度上依赖于系统网络链路的物理安全。因此，必须保护系统链接的完整性，防止外部代理人的非法连接。

解决方案:

SMART PATCH面板系统

智能接线板系统允许用户控制网络中使用的所有链路的结构。智能配线架可以监控和控制网络及其各个组件的功能，并确保链路正常维护，网络功能齐全，所有网络连接都是安全的。

与传统布线系统相比，最大的差异之一是智能补丁系统能够轻松地将某些链接指定为“机密”，允许管理软件将网络设备分配到某些MAC地址，并确保仅允许指定的设备进行接口用这个连接。

如果发生非法连接，或连接中断，系统将发出警报通知。该功能远远超出了传统布线系统的能力，对系统的整体安全性有重大影响。

智能补丁系统也能够与其他安全系统（如监控系统）集成。例如，如果智能配线架系统注册连接错误，则监视系统可以通过接线板安装的摄像机提供事件的视觉确认。

Data Center Security Solutions

风险9:

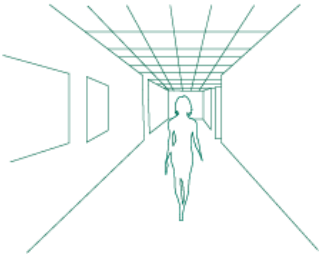
黑客

在公司越来越依赖电子数据的时代，由于外部黑客造成的安全漏洞是一个主要的漏洞。虽然IT安全对黑客的保护影响最大，但物理安全系统也可以在防范组织免受外部攻击方面发挥作用。

解决方案:

整合物理访问,管理和登录系统

将物理访问管理系统与登录信息系统集成确保仅允许通过访问控制系统进入计算机室的用户登录到服务器。



Data Center Security Solutions

风险10:

无效存货管理

保存数据中心硬件的清单通常由员工完成，通过扫描设备序列号或其他方法。在这种情况下，员工工作量增加，错误常见。

员工必须在整个数据中心完成对设备的检查，并在数据库中保留详细的记录。管理可移动IT资产的工作量和风险特别高。例如数据磁带的丢失，是数据中心管理人员头痛的一个。

解决方案:

RFID资产管理系统

使用RFID技术，员工在进行检查时只需携带RFID阅读器设备，并可立即识别哪些设备位于什么位置，以及是否丢失任何设备。该技术还可以提高库存记录的准确性。

金融服务行业公司和任何其他需要进行定期审核以确保IT基础设施设备安全的公司，库存准确性是一个特别敏感的问题。如果一家银行无法找到其服务器，那么对其业务的影响将至关重要。

租赁硬件的IT经理可以从RFID资产管理系统获得重大收益，因为它们能够确定哪些设备项目正在使用中，哪些设备闲置以更有效地控制成本。

此外，RFID阅读器可以由数据中心入口点安装，如果从数据中心取走任何硬件，可以发送通知。

Data Center Security Solutions

其他考虑的系统：

- *人脸识别系统*
- *视频分析*
- *反恐怖装置*
- *安全检查设备*

有任何其他问题吗？点击这里
通过我们的网站联系我们！

www.cd-estt.com