

简译版

2021 年数据中心弹性将更加重要

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	2021 Will Be the Year of Data Center Resiliency: Plan Now		
原文作者	汤姆·基布林 (Tom Kiblin)	原文发布日期	2020 年 12 月 10 日
作者简介	汤姆·基布林是 ServerCentral Turing Group (SCTG) 托管服务的副总裁。		
原文发布单位	Network Computing		
原文出处	https://www.networkcomputing.com/data-center-s/2021-will-be-year-data-center-resiliency-plan-now		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antivy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公有方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 		

2021 年数据中心弹性将更加重要

汤姆·基布林

2020 年 12 月 10 日

弹性 IT 系统（可以在电力中断、恶劣天气和安全事件中保持可用性的系统）一直是企业弹性的关键组成部分。

数据中心是许多企业 IT 环境的基石，这些物理存储站点依靠强大的连续性和灾难恢复计划，在发生攻击的情况下支撑业务运营。

新冠疫情爆发后，企业意识到他们在大规模转向远程办公时缺乏全面的连续性计划，因此他们开始紧急制定数据中心弹性计划。在各行业中，网络攻击继续呈上升趋势——今年第三季度，我们记录了近 300 起勒索软件攻击，是上一季度的两倍。

IT 领导者应立即采取行动，增强其数据中心的安全性，以应对来年严峻的安全威胁。2021 年，企业在制定数据中心弹性计划时需要了解下述内容。

根据应用程序的重要性确定弹性目标

有关数据中心弹性服务的问题在于，它们通常为所有企业推荐同样的“弹性”端点。而现实情况是，对于每个企业而言，在发生攻击时出现的问题和所需的服务都会有所不同。

在理想情况下，发生攻击时所有应用程序仍保持可用状态，或者其恢复时间少于一个小时。但是对于大多数企业而言，技术或经济限制使得上述场景无法实现。应用程序可能太过复杂，无法重新编码以在多个数据中心中运行，或者这样做可能要花费数月和数百万美元。

在确定数据中心弹性的目标时，企业必须区分对业务至关重要的应用程序和非重要应用程序。这有助于最大程度地减少经济和生产损失，并为需要最大弹性的系统预留资金和资源。

例如，人力资源应用程序可能不需要小于 24 小时的“恢复时间目标”（RTO），因为这类应用不会严重影响日常运营。与此相反，支付处理器可能需要在几个小时内恢复，以维持持续的客户服务。

设备可见性的降低更凸显了数据保护的必要性

IT 领导者对员工设备的可见性有限，这增加了远程办公的安全风险。远程员工更容易出现人为错误，使未打补丁的数据和资产更易遭受恶意软件的攻击。

但是，并非所有数据都有同样的重要性。正如企业必须优先考虑关键应用程序以进行弹性规划一样，IT 领导者也必须识别最敏感的数据集，例如包含客户或机密信息的数据集，以进行弹性资源规划。

在保护敏感数据免受恶意软件威胁方面，预防和快速恢复是两个重要组成部分。IT 领导者可以通过以下两种方式制定弹性计划。

- **员工培训。**企业应重视员工培训。IT 领导者应向员工分发培训材料，告知其如何检测和报告网络钓鱼活动或勒索软件攻击等威胁。
- **不可更改的备份。**如果备份未进行锁定，那么它们在数据恢复方面基本就是无用的。存储在数据中心的不可更改备份，能够保护遭泄露的数据免遭篡改。

借助云增强数据中心的弹性

虽然疫情和远程办公环境给业务和数据中心连续性带来了新的挑战，但是企业可以采取已有的解决方案和策略。例如，数据中心和云的混合就是一种动态弹性方法。

至于关键应用程序和敏感数据集分别应存储在哪里，企业可以参考下述准则。

- 传统、非弹性和静态应用程序存储在数据中心。这些应用程序难以进行重组，无法存储在云中。
- 高度敏感的数据集存储在数据中心。数据中心更有利于满足严格的监管和合规性要求——如果执行不当，这些资产的云迁移可能会带来风险。
- 高使用率的应用程序可以存储在云中。大量员工使用的关键应用程序（例如薪资应用程序）在云中更易扩展。

不要在发生攻击后才开始建立数据中心弹性

通常，只有在出现真正的攻击并损害业务连续性时，企业才会评估其数据中心的整体弹性。

现在，IT 领导者应该针对最坏的攻击情况进行计划，以提高他们在这种情况下的响应能力。他们可以通过对关键应用程序和敏感数据进行优先级排序、员工培训、恢复和备份计划以及云增强来实现此目的。这样一来，企业就可以做好准备，顺利应对 2021 年可能发生的攻击。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队,始终坚持自主先进的能力导向,依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累,研发智甲、探海、镇关、捕风、追影、拓痕等系列产品,为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系,依托全面持续监测能力,建立系统与人员协同作业机制,指挥网内各种防御机制联合响应威胁,实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合,协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设,支撑起协同联动的实战化运行,赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方,全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴,目前,安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点,在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面,实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体(如 APT 组织)及其攻击行动,进行持续监测和深度解析,协助客户在“敌情想定”下形成有效防护,通过深度分析高级网空威胁行为体的作业能力,安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可,已连续六届蝉联国家级安全应急支撑单位,是中国国家信息安全漏洞库六家首批一级支撑单位之一,亦是国家网络与信息安全信息通报机制技术支撑单位,国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日,在习近平总书记主持召开的网络安全和信息化工作座谈会上,安天创始人、首席架构师作为网络安全领域发言代表,向总书记进行了汇报。2016 年 5 月 25 日,习近平总书记在黑龙江调研期间,视察了安天总部,并对安天人说,“你们也是国家队,虽然你们是民营企业”。

安天实验室更多信息请访问:

<http://www.antiy.com> (中文)

<http://www.antiy.net> (英文)

安天企业安全公司更多信息请访问:

<http://www.antiy.cn>

安天移动安全公司 (AVL TEAM) 更多信息请访问: <http://www.avlsec.com>