

简译版

防火墙无法保护企业数据的八个原因

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	8 Reasons Perimeter Security Alone Won't Protect Your Crown Jewels		
原文作者	胡安·帕勃罗·佩雷斯·埃切戈延 (Juan Pablo Perez-Etchegoyen)	原文发布日期	2020 年 9 月 16 日
作者简介	胡安·帕勃罗·佩雷斯·埃切戈延是 Onapsis 公司的首席技术官。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/cloud/8-reasons-perimeter-security-alone-wont-protect-your-crown-jewels/a/d-id/1338878		
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.antiy.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。 		

防火墙无法保护企业数据的八个原因

胡安·帕勃罗·佩雷斯·埃切戈延

2020 年 9 月 16 日

大多数防火墙和安全设备可以有效地保护系统和数据，但是它们能保护关键应用程序吗？

如今，全球大企业都依靠特定技术来运行其日常业务，而这些业务均由关键任务应用程序支持。这些应用程序，如企业资源计划(ERP)、供应链管理(SCM)和客户关系管理(CRM)应用等，由 SAP 和 Oracle 等供应商提供。它们经常需要处理企业最敏感、最有价值和受监管的数据。

运行关键任务应用的企业很有可能在网络上部署多个防火墙。这些防火墙可以保护其基础架构，为所有应用提供基本的安全保护。但是，关键任务应用非常复杂，要想充分保护它们，企业需要部署专门的流程和技术。

现在，很多企业开始进行数字化转型或云迁移，这会导致更多的应用（例如手机应用和集成的多重云环境）能够访问其高价值数据，增加数据泄露的风险。在许多情况下，这种级别的可访问性还会允许用户从不受信网络（通常是互联网）下载应用。

即使企业部署了防火墙，其业务应用也会面临数据泄露威胁。下面，我们将介绍八种威胁情况。

1. 恶意员工/内部人员威胁

企业员工通常能够访问关键任务应用，以便执行从报销差旅费到创建供应商等流程。企业员工已经具备了执行某些任务的权限；相比于其他攻击者，他们更有优势。他们可以利用这些权限来提权，执行其他未经授权的活动。如果员工具有特殊权限（即开发权限、系统管理员授权等），这种风险就更加严重了。

2. 受感染账户和凭证

通常，用户每天都会使用同一登录机制进行身份验证，以登录业务应用。如果攻击者窃取了其登录凭证，就可以访问关键任务应用了。攻击者试图感染具有高级权限的用户（例如系统管理员），以便迅速提权。

3. 受感染端点

企业员工从各个端点连接到业务应用。在很多攻击中，攻击者使用恶意软件或恶意代码感染端点，以劫持操作系统和用户账户。鉴于此，企业开始关注端点安全问题。一旦端点受到感染，攻击者就可以直接与关键任务应用建立连接，从而感染多个用户账户。

4. 网络钓鱼攻击

网络钓鱼攻击主要通过电子邮件传播。攻击者将恶意代码传递给企业，诱骗员工执行恶意活动。这种攻击方法非常有效。攻击者使用该方法来感染端点或用户账户，然后再连接到内部应用。

5. 集成和多重云环境

业务流程跨多个系统执行，需要进行数据整合和集成。关键任务应用通过接口与其他应用和企业互连。攻击者可以利用这些接口进行横向移动，攻击其他系统和应用程序，以感染最关键的应用。此外，随着云迁移和数字转型计划的发展，许多关键任务应用正在迁移到云环境。在某些情况下，这些应用可通过互联网下载，这又增加了一层复杂性和潜在攻击面，攻击者可以利用这些攻击面来访问关键业务应用。

6. 业务合作伙伴和供应商访问

在大多数情况下，企业提供 VPN 连接或对合作伙伴、供应商或外部承包商的访问。此外，由于企业对关键任务应用的持续可用性具有严格的要求，因此供应商需要部署一种机制来监控支持这些应用的技术。SAPRouter 就是一个很好的例子。对于 IT 团队来说，它通常是未知的，但它提供了互联网与企业 SAP 应用之间的连接。如果配置错误或过时，它可能会被滥用，转而提供互联网与业务应用的连接。通过 SHODAN 进行被动搜索显示，目前约有 11,000 个 SAPRouter 暴露于互联网。

7. 移动应用程序

现在，大多数业务应用支持某种形式的移动访问，包括专用移动应用到支持移动功能的用户界面框架，例如 SAP Fiori。这进一步扩大了攻击面，不仅移动应用会成为攻击目标，移动设备也会成为攻击目标。

8. 面向互联网的应用

在许多情况下，企业的 IT 安全团队认为其关键任务应用不会暴露于互联网，但是他们

通常无法获得 SAP 应用运行方式或安全性的可见性。SHODAN 搜索显示，成千上万个业务应用直接连接到互联网，这大大增加了攻击面和风险。攻击者可以将这些应用用作直接入口点。举例来说，2016 年 5 月，US-CERT 发布了第一个关于 SAP 应用网络攻击的告警 (TA16-132A)；最近又发布了一个告警：Netweaver AS Java 的严重漏洞。

企业应该怎么办？

在当今的环境中，关键任务应用更加暴露，它们连接到多个网络和应用。即使企业的关键任务应用受到防火墙的保护，但是它们还面临许多其他风险，攻击者可以利用这些风险窃取企业的高价值数据。这进一步说明，企业需要部署专门技术来保护关键任务应用，并提供适当级别的可见性，以及检测和预防控制措施，以保护企业最重要的信息和流程。

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>