Universe Scientific Publishing
Computer System Network and Telecommunications,计算机系统网络和电信(1) 2019,3
ISSN: 2661-3719(Print) ISBN:2661-3727(Online)

基于云服务在企业的安全风险探究

赵祖立 唐宾徽
四川大学锦城学院 计算机与软件学院 四川 成都 611731

DOI: 10.18686/jsjxt.v1i3.1282

【摘要】SaaS 云服务已经深入企业的应用环境,本文首先阐述了 SaaS 服务的基本概念,并针对客户企业在使用 SaaS 服务的过程中面临的诸多安全风险进行分析,提出一些影响客户企业的安全风险的因素,目的是提高企业在使用的云服务的同时提高安全意识。

【关键词】云计算;安全风险; SaaS 云服务

1 SaaS 服务系统概述

SaaS:Software-as-a-Service(软件即服务),它是以互联网为依托的新型的软件应用模式。运营商可以提供给客户企业运行在云计算基础设施上的应用程序,客户企业可以在各种设备上通过客户端界面访问。企业可以结合自己实际需求通过厂商定制需求获得相应的软件服务,按需付费。相比传统的购买软件,企业节省了前期大量的软件系统的购置或研发费用,通过租用运营商 Web 软件,企业不需要进行后端维护,节省大量的人力资源和成本,使企业专心于核心业务并提高工作运行效率。

服务提供商整合了庞大的计算机软硬件资源,通过互联网对外提供业务服务。SaaS 模式通过多租户的架构使用虚拟机技术为每个租户分配合适的软硬件资源,服务商可以不断更新基础设施的配置,更方便了设备后台工作人员的解决问题和对设备的维护,也节约了客户企业软件升级的成本费用。

从技术角度看、随着 API 调用越来越多,跨层应用也越来越多,例如统计类工具,SDK 部分是在 PaaS 层完成,但后期所有的报表查看和分析都是在网页端(SaaS 层)完成。[1]]SaaS 层在云计算的分布层次如图:

云计算层次图

1.1 SaaS 服务的特征

1.1.1 按需分配:在:SaaS 模式下,用户可以根据自己的需求"量身打造",让软件服务根据有灵活性,SaaS 供应商可以根据客户需求将软件应用的各个模块进行重新组合,形成用户个性化的需求的软件服务。

1.1.2 多租户架构: SaaS 模式的多租户架构就是 SaaS 供应商以较低的开发成本设计一套标准化软件系统,并提供给成千上万的用户使用,一次来实现软件服务的规模效应。[2]

1.1.3 网络特性: SaaS 服务是以网络传输的手段为客户提供服务,在 SaaS 服务中也呈现了许多的网络技术的特性,客户企业可以通过 web 浏览器或者专业的客户平台通过网络与服务器交互,大量的数据处理操作都还在服务器端进行处理,最终把需要的结果通过网络传输返回给客户端。

1.1.4 可编程的特征: SaaS 供应商可以使用 API 对云计算资源进行创建、修改,也可以通过 AWS cloudForom 等代码工具对云资源进行编程,通过编程的方式进行自动化的管理,比传统的数据中心更快速的反应监控配置的错误和偏差,提高快速自我修复能力,保护一些重要敏感的数据。

2 企业面临的安全风险分析

2.1 安全风险来源

2.1.1 黑客:通常利用专业的计算机及网络技术对攻击目标计算机或服务器,对企业有较高的经济价值的数据进行窃取。黑客对 SaaS 服务攻击的威胁常常出现在数据在广域网的传输过程中。

2.1.2 计算机病毒:病毒是在云计算的环境下的重要隐患,一旦运营商或者企业感染了病毒将会降低计算机系统的运行效率,甚至会造成整个系统的瘫痪。如蠕虫病毒,木马病毒,脚本病毒等等。

2.1.3 内部人员:内部人员拥有数据管理的部分权限,少数员工利用职业便利窃取数据从而获得经济利益,而且内部人员的安全风险是难以控制因素之一。

2.1.4 物理灾害:计算机的物理威胁包括人为的物理灾害、自然灾害、环境事故以及人为的误操作,

ISSN: 2661-3719(Print) ISBN:2661-3727(Online)

其中一些火灾、鼠害、雷击和地震等自然灾害都通常都是无法规避的风险。

2.2 安全风险因素

2.2.1 数据风险

数据对企业是极其重要的,它对于企业起着至关重要的作用,当企业的数据一旦遭受破坏时,将会对企业造成不可估量的损失。如果运营商未能及时采取补救措施恢复数据。客户企业极有可能将会面临被市场淘汰的风险。因此,网络安全中保证数据安全是 SaaS 服务的重要问题。

2.2.2 数据锁定风险

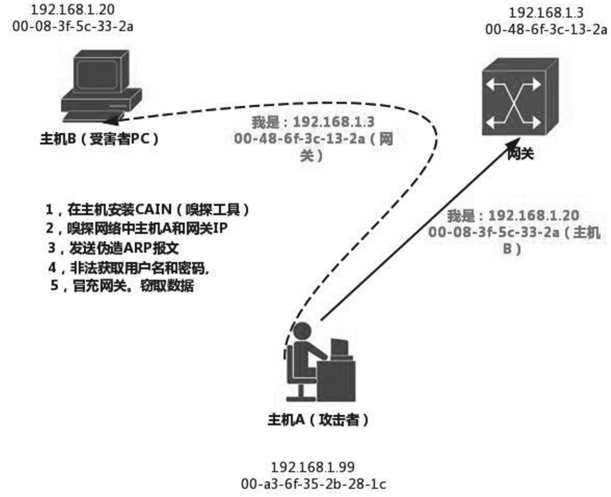
由于企业未能拥有完全的数据掌控能力,企业将会面临由于黑客、市场竞争等多方面的原因数据遭到锁定的风险。在 2017 年 1 月,MongoDB 公司爆发了数据库勒索事件,多达 33000 个数据库遭到非法入侵,数据库的数据被黑客洗劫一空并留下要求支付比特币赎回数据的勒索信息。

2.2.3 数据的非法使用

数据对企业企业启正至关重要的作用,其中存储着企业的财务、管理、产品等重要数据信息,还有极高的商业价值的客户信息的数据。在 SaaS 模式下,数据存储的物理介质在服务供应商处,企业无法完全控制数据的物理存储介质的功能,因此企业将会担心核心数据遭到供应商的非授权使用。

2.2.4 数据传输风险

在 SaaS 的模式下,数据都是通过网络传输的手段进行信息的存储交互,在数据传输的过程中的经常会遭到非法的网络攻击,在网络不断发展的今天,网络攻击的事件频频出现,诸如 DDOS、ICPM 泛洪攻击、TCP/UDP 泛洪攻击和 ARP 攻击等等,这些都是数据在网络传输的过程中遭到非法入侵。如攻击者通过发送伪造的 ARP 报文,恶意修改网关或网络内其他主机的 ARP 表项,造成用户或网络的报文转发异常。下图是 ARP 欺骗攻击流程:



ARP 欺骗示意图

2.2.5 数据篡改

企业把数据传送给服务提供商后并不知道供应商是如何进行数据处理的,企业不知道的数据是否在后台被修改,所以客户企业将面临数据在存储的完整性的风险。

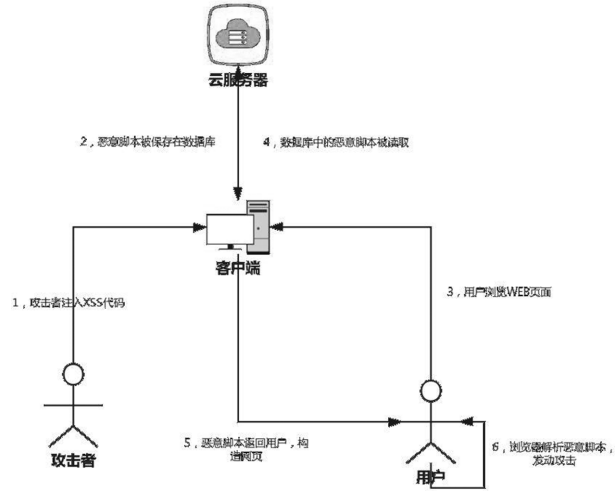
2.3 物理安全

又称为硬件安全,其中包含的基本要素:电源、基础设备、通讯设施、SaaS 服务提供商的系统环境等等。由于所有的 SaaS 服务的资源都存储在服务提供商的服务器上,而且必须全天候的提供服务。所以在遇到自然灾害、系统崩溃等都会对 SaaS 服务的数据和隐私在成极大的威胁。就在 2018 年 4 月 21 日陵城。云计算提供商 Amazon(亚马逊)公司出现了大规模的宕机事件,导致向客户提供的新闻服务 Reddit、位置跟踪服务 FourSquare、回答服务 Quora 等网站受到了影响,由于亚马逊的云服务中断导致客户 Reddit 网站的服务能力下降持续了近 4 天,造成客户企业巨大的损失。

2.4 客户端的风险

由于现在的 SaaS 服务多采用面向浏览器的和服务器的 B/S 架构,在广域网的环境下,对客户端的安全有非常多的隐患,而且目前的客户端浏览器也存在一些漏洞,如 SQL 注入、跨站脚本攻击、HTTP 爆头追踪,若客户端遭到攻击,在用户输入数据时信息就会被窃取,相应的服务器也不可避免的受到影响,最终会企业在成严重危害。因此 SaaS 模式的独特性让客户端出现安全问题时会造成不可估量的大范围的影响。

比较常见的跨站脚本攻击漏洞(XSS 漏洞),攻击者通常会通过站点的一些留言功能、评论功能或电子邮件功能向用户插入一个指向恶意 URL 的链接,当用户在 web 浏览器打开 URL 链接时恶意脚本就会被解析,[3] 从而达到攻击目的。攻击流程如图:



XSS 攻击流程图

ISSN: 2661-3719(Print) ISBN:2661-3727(Online)

2.5 账户权限问题

在 SaaS 的模式下,服务商掌控着所有账户的超级权限,所以,在被授予客户企业账户权限变更时需要服务商的超级用户的手动处理权限,当企业掌握重要权限用户的员工离职等情况,在未能及时的账户的注销变更,若离职员工通过旧账户依然具有资源管理权限,将会严重威胁到企业的数据安全。

2.6 人员操作不当

企业在使用 SaaS 服务时,超级用户手动给客户企业一定的管理数据资源的权限,并发放给相关的管理人员,拥有高级权限的使用者必须有专业的相关知识,若出现重大的操作失误将会干扰的到服务器系统的安全运行。

2.7 战略风险

由于 SaaS 服务的特征,企业需要结合信息技术等外包业务,对整个企业的内部的资源部署、组织架构和业务处理流程做出适当的调整,使企业失去对部分资源的控制能力,对企业品牌认知、企业文化、战略规划都产生影响。由于软件开发、信息处理技术的外包导致企业缺乏 IT 创新能力,对于部分拥有庞大用户量的企业,供应商所提供的的外包应用软件、基础设施和边缘服务,将会降低用户对企业品牌的信心,甚至影响企业的服务可用性和服务体验。

2.8 成本增加的风险

企业采用 SaaS 服务最直接的驱动就是成本因素,虽然 SaaS 模式可以让企业在信息建设初期节约大量成本,但是,对于企业长期的战略角度,随着企业需求不断扩大,企业不断增加的个性化和弹性需求,以及 SaaS 供应商为客和提供的电话、培训支持和各类的隐形成本,将会不断的增加边际成本,最后企业将重新采用传统的模式,到那时信息管理系统建设将会有非常大的难度和资金投入。

2.9 法律风险

由于法律在科学技术方面生具有一定的滞后性,传统的租聘模式的法律法规已经逐渐不适用新型的 SaaS 模式,其相关的合同法、租赁法等相关法律法规已经不健全将会导致法律纠纷。SaaS 模式下的软件传播和许可使用方式在技术特性和商业模式有了新的发展,在软件著作权人、云服务提供商和云用户三个主体之间隐含着著作权的若干可能。[4]

由于云计算发展迅速,目前未能形成权威的第三方认证机构,也未能形成一套健全、权威、公正的监督管理体制。所以企业和运营商进行商业运行时很难有可靠的基础和安全保障。就如在 2018 年的亚马逊云服务宕机事件中,服务提供商在法律上却没有违反亚马逊 EC2 服务的服务等级协议(简称 SLA),由于出现故障的是 EBS 和 RDS 服务,而不是 EC2 服务,所以是客户和服务提供商真正受保护的不仅仅是类似这种的协议保证,而是强有力的技术规范和合同保障。

3 企业应对安全风险的防护

3.1 采用分权分级的管理模式

根据不同的安全级别的人有不同的管理权限,一些重要的数据操作人员在进行数据操作时要严格遵守规章制度和流程,并对操作进行详细的日志记录。防止由于权利过于集中,减少少数人在经济利益的趋势下进行数据盗窃的事件。

3.2 建立网络访问控制系统

3.2.1 访问控制系统可以对企业重要的权限控制、属性控制和网络访问进行控制,限制不同等级的用户的访问权限,禁止未经授权的操作。

3.2.2 部署防火墙对系统,内外网进行隔离,对敏感或有害的数据进行拦截,防止数据泄露在传播到外网,对企业和用户数据安全都起到非常重要的作用。

3.2.3 实时监控,利用过滤器(Vericept 或 Websense)技术随时监控用户数据传输或远程操作过程,一旦发现可以数据或者非法入侵破坏行为进行及时过滤和拦截,防止木马病毒的攻击和用户数据泄露。[5]

3.3 建立云安全防护系统

在客户端也要进行一定的网络安全防护,其进行保护的方法有两种:其一,设置防火墙,并安装杀毒软件,当计算机受到木马或者病毒攻击时杀毒软件会进行预警提示,可以有效的保护计算机的安全,阻挡非法入侵。其二,利用端口扫描工具或者检测软件对信息接收系统进行监控,若有非法入侵及时切断网络。[6]

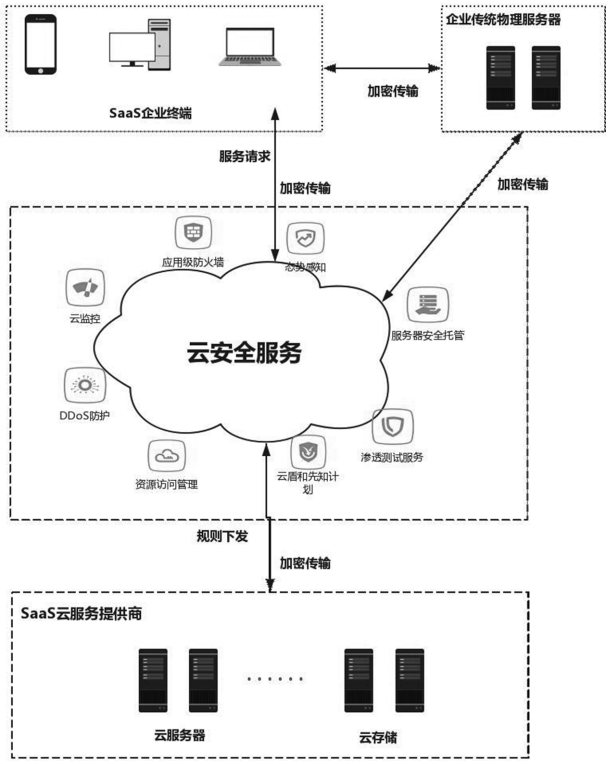
3.4 对数据加密处理

计算机网络技术中的保密性通常利用物理手段和数学手段达到在传输信息、存储信息的过程中信息不回造成泄露的目的,这是一种主动性的防范信息安全问题的措施。[6]使用 DES 数据加密标准和 RSA 体制的结合,在数据传输前进行加密处理,在数据到达接收点时对密文进行解密,保证数据在网络传输的过程的安全。

3.5 建立云安全防护系统

黑客攻击通常下会造成大量的经济损失,所以建立完善安全防护系统是非常有必要的。企业可将利用云安全一站式的云安全产品和服务,以大数据平台为基础实现检测、防御、审计和事件响应综合化的全面的安全防御体系。下图是云安全防护系统模型:

ISSN：2661－3719(Print)　　ISBN:2661－3727(Online)



3.6　提高内部人员的安全教育和培训

通过定期的安全培训，不断规范内部员工的管理工作，并深化员工的职业操守和职业道德，加强相关法律规章的安全教育。员工还要不断学习云计算的新技术，关注网络安全知识的发展，树立网络安全防范意识。

4　结束语

总而言之，在互联网高度发达的今天，网络安全在云计算的应用中处于一个非常突出的问题，客户企业在享受 SaaS 云服务带来的便利时，更要重视数据存储传输的各种风险，在树立长远的战略目标时要意识到企业独立的信息系统的建设的重要性。客户企业应该积极主动的面对企业在发展过程中遇到的各种安全风险问题，增强企业的综合实力，提高竞争力。

【参考文献】

[1]. 2016 年中国企业云服务市场规模超 500 亿[A]. . 艾瑞咨询系列研究报告(2017 年第 6 期)[C]. :上海艾瑞市场咨询有限公司,2017:8.

[2]赵智鹏. 面向 SaaS 业务的平台型商业模式成型中的合法化问题与对策研究[D]. 东南大学,2018.

[3]孙国栋. XSS 漏洞攻击与防御研究[D]. 辽宁工业大学,2018.

[4]郭鹏. 云计算 SaaS 模式下的著作权侵权分析[J]. 知识产权,2018(11):52－59.

[5]王晓妮,段群. 基于云计算的数据安全风险及防御策略研究[J]. 计算机测量与控制,2019,27(05):199－202＋225.

[6]金路. 基于云计算下计算机信息安全与保密分析[J]. 网络安全技术与应用,2019(05):32－33.