SaaS 开发指南——安全篇

SaaS 开发指南——安全篇

最近，云计算不断升温，吸引了众人的眼球，对 SaaS 技术的热烈讨论渐渐平息。平淡的背后其实是技术的不断积累和沉淀，SaaS 技术在不断走向成熟，在 SaaS 模式下，应用通过互联网交付到客户端，用户直接选择并使用需要的软件，而不需再去购买软件许可，安装并维护软件，取而代之的是向云服务供应商支付使用费用。信息安全问题一直是 IT 行业不得不面对的问题，SaaS 技术也逃不出这个魔咒。

SaaS 开发信息安全事件

各大企业的首席信息技术官（CIO）和首席安全执行官（CSO）们一致认为，公共云端最大的安全疑虑就是：“其他客户可能会看到我的数据。” 企业若采用 SaaS，通常就无法使用异地密钥来将数据加密，而且也无数据外泄预防(DLP)或是许多其他企业级的安全方案可用。现在，SaaS 厂商的信息安全事件已经实际印证了这项疑虑。

- **微软数据外泄事件突显 SaaS 安全问题**

SaaS 开发安全问题分析

对于探寻选择 SaaS 的公司来说，安全性始终是最大的难题。不论你的加密强度有多大，或是应用哪种类型的加密，一些潜在的客户如果得知自己的数据处于他们自己无法管理的异地，并且他们的数据可能就在竞争对手的数据旁边，他们还是会彻夜难眠。

- SaaS 对数据安全的影响
- 用户发现 SaaS 安全隐患
- SaaS 安全性的两种声音 我们该相信谁？

化解 SaaS 安全问题的措施

在面临软件即服务 SaaS 应用中的安全性问题时，密码管理不当和不安全协议威胁都将会对您的系统保密造成破坏或数据泄露，同时可能需要由您的企业来承担法律责任。面对 SaaS 所带来的安全威胁，我们应该怎么做才能够减轻这些威胁？

- 化解 SaaS 安全问题的三大措施
- SaaS 有关的安全技术
- 告别“纸上谈兵” 如何建立安全的 SaaS 服务？
- SaaS 安全与应用探讨

微软数据外泄事件突显 SaaS 安全问题

据 PCWorld 报导，微软云端商业软件包 BPOS 发生客户数据遭该软件其他客户存取并下载的事故。

Google、微软以及数不清的其他 SaaS 供货商，都曾发生过资料外泄事件。比较起来，这一次还算是轻微的：一位应该是微软的员工，因为组态设定的错误而产生一个全局性的漏洞。还好，微软自行发现了这个问题，并且在 2 小时内修正了问题，而且外泄的数据也还算无害。不过，事故毕竟发生了。

在最近的 Gartner Data Center Conference 数据中心大会上，挤满演讲厅的一大群首席信息技术官（CIO）和首席安全执行官（CSO）们一致认为，公共云端最大的安全疑虑就是：“其他客户可能会看到我的数据。”现在，多家 SaaS 厂商的信息安全事件已经实际印证了这项疑虑。

CIO 们必须在 SaaS 和 IaaS 之间作取舍，前者对 IT 部门来说是很方便，但存却在着应用层级的分租共享风险，而后者虽然有许多环节可以建置数据加密方案，但 IT 部门的营运负担较重。我预测，在未来几年，规模较大的 IT 部门将开始采用 IaaS 来建置大型的云端项目，理由正是因为 IaaS 能提供比 SaaS 更多的安全控管。

企业若采用 SaaS，通常就无法使用异地密钥来将数据加密，而且也无数据外泄预防(DLP)或是许多其他企业级的安全方案可用。

看来，SaaS 供货商有必要大幅改善其透明度以及信息安全能力的广度。如果厂商无法证明他们如何追踪组态变更，或是无法预防组态设定错误，大型的 IT 部门根本就不会将某些数据交给这些厂商代管。

不过，话说回来，如果您因为组态设定的错误而导致 Exchange 通讯簿外泄，您自己的 IT 部门是否有办法在二小时内发现并修正问题，就像微软这次的案例一样？如果您的 IT 部门规模不大，SaaS 供货商的安全措施，尤其是微软、Google 或 Salesforce.com 这类的大型供货商，或许会比您自己的作法更安全也说不定。

查看原文

SaaS 对数据安全的影响

对于探寻选择 SaaS 的公司来说，安全性始终是最大的难题。不论你的加密强度有多大，或是应用哪种类型的加密，一些潜在的客户如果得知自己的数据处于他们自己无法管理的异地，并且他们的数据可能就在竞争对手的数据旁边，他们还是会彻夜难眠。

Iron Mountain Digital 公司总裁 John Clancy 承认“数据安全性始终是他们选择 SaaS 的主要障碍。但是，和以前相比，这些障碍还是比较容易克服的。”他补充到“这些公司使用和联邦政府同等的加密”。

Gartner 公司的首席研究分析师 Adam Couture 表示像 EMC 和 IBM 公司很好的帮助客户解决了后顾之忧。他们在网上将数据传输到远程主机设备上。Couture 说：“他们并不是将数据送到 Mozy，但是最后会将其送到 EMC Mozy。对我来说，这二者之间有很大的不同——存储 OEM 厂商希望自己成为服务供应商”

在网上备份空间里，Perimeter eSecurity 并不像希捷的 EVault 或者 Iron Mountain 甚至 Incentra Solutions 公司或 Intronis Technologies 公司那样有

名。但是 Perimeter eSecurity 公司战略领导 Doug Howard 表示，他们进入该领域主要是为了和那些不是经常进行加密业务的公司相竞争。

他说，“你会发现大多数在线备份供应商都可以在这些一个密钥的基础之上选择加密。但是我们做两个主要密钥，这也就意味着每个加密有两个密钥。你可以选择让某些人对信息有限制访问，因此不能访问所有的文本或 word 文档，但是你可以看到页眉或文件名。这就赋予了你很大的灵活性。大多数供应商都为客户提供了可选方案，客户既可以自己保管密钥，也可以交给第三者由 SaaS 供应商保管。

James Cosgrove 是总部坐落在西雅图的 Computer Resource Corp(CRC)公司的创始人并担任公司的 CEO。他选择让 Intronis Technologies 掌握他的密钥。“理由是如果其中一个小小的密码丢失或错位，我们就丢失了客户数据。”他的客户大部分都是西雅图地区的牙科诊所。在他们采用在线备份策略时，他们用的是赛门铁克的备份工具。他说“他们可能会说这些磁带脏了，或者说在晚上不备份，我们对这些电话已经感到厌烦了。”

查看原文

（作者：Ellen O’Brien　　译者：杨君　　来源：TechTarget 中国）

用户发现 SaaS 安全隐患

软件服务可能是目前最热门的有关网络存储技术的技术之一，但是用户却依然不放心将自己的关键数据保存在自家以外的地方。用户发现 SaaS 安全隐患问题。

"我们只是感觉将数据放在外面很不舒服，为了让他们更加安全我们要将他们保持在公司内部。"位于乔治亚州的贝里学院的首席信息安全官 William Souder 表示，"我们的数据对于家庭教育权和隐私法以及健康保险流通与责任法案是如此的敏感，这些法案约束着我们的数据。"

目前，包括 IBM、Google、戴尔和 EMC 公司等众多厂商都加入到了 SaaS 的行列中，无论其形式是以云计算、电子邮件服务还是在线备份服务的形式。

不过，贝里学院的 Souder 表示，他也不排除在未来的某个时候考虑 SaaS，但是他同时还表示，他需要一些令人信服的理由才会去部署 SaaS 服务。

"我可以把我的数据交给第三方，但是卖方必须通过相应的认证，因为我们不得不考虑经由广域网传输数据的各种情况。"Souder 表示。

不仅仅是教育部门的数据在被精心呵护着并对 SaaS 不感冒，另外一个健康保健组织的数据也对 SaaS 十分紧张。

"我们在内部能够掌握所有的东西。"一家位于佛罗里达州的卫生保健服务提供商的不愿透露姓名的 IT 经理表示，不过他补充到，"安全是一回事，但成本也是一大需要考虑的因素。"

惠普是最新加入到 SaaS 阵营当中的厂商，在昨天惠普发布了其在线存储服务 HP Upline。

不过，从用户的角度看起来，厂商要想说服用户采用 SaaS 仍然需要做许多工作。

"从供应商方面，已经有太多的关于 SaaS 的说法了。"IDC 分析师 Doug Chandler 在发言中表示，他并不建议用户在进行了广泛的调查之前迁移到 SaaS 服务上去。

"你应该确保供应商明白你所关注的地方，他们使用什么类型的加密技术？他们已经为自己的数据中心应用了何种程度和类型的安全服务？"

总之，用户必须考虑涉及 SaaS 部署的所有可能出现的情况，包括可能发生的时候，你与供应商之间的关系。

"很多人没有考虑到如何从 SaaS 服务中全身而退。"Doug Chandler 表示，"如果合同结束了，你怎么才知道你的 SaaS 服务提供商已经彻底销毁了所有的你的数据备份。

查看原文

（作者：James Rogers）

SaaS 安全性的两种声音 我们该相信谁？

随着 SaaS（软件即服务）越来越火热，SaaS 的安全性是成为被用户、厂商和媒体激烈讨论的话题。

安全性的两种声音

有人说：SaaS 模式的数据存储在公网上，掌握在 SaaS 服务商的手上。而且，黑客可能破解并进入数据服务器，获取数据，这听起来好像有些道理。有人甚至说：使用 SaaS 软件时，很容易把病毒带到公司的内部网络，甚至把病毒传染到其他服务器，这无形中给公司内部网络带来隐患，这是“耸人听闻”吗？

另外有一种声音就是 SaaS 实际上提升了信息化系统的安全性，因为安装在局域网的软件系统也面临一些安全的问题，比如：

1、解决对软件商、服务商的信任问题。

大多数客户不能完全百分之百的完成系统的维护，此时厂商提供服务时，厂商的技术人员一样可以很方便的接触到用户数据。

另外，安装在客户局域网的系统升级的时候，都是由局域网内部服务器发起访问外网，此时内网外网对于开发厂商来说是透明的，这也存在用户对软件服务商的信任问题。

据统计，信息化系统的安全威胁 90%都来自局域网内部，可怕的黑客病毒或木马程序的危害远远大于服务器被攻破；比如 Arp 欺骗导致内网全数据泄密，利用 Arp 欺骗而传播的病毒，黑客可能能加容易进入核心的数据服务器。

2、解决对内部信息系统维护人员的管理和信任问题。

内网需要专门的人员和设备来解决信息化的问题，因此存在系统维护和设备维护，一般来说，内网系统由于人员上的安排和水平是否能做到很好的数据备份或异地数据备份呢？当发生重大恶性事故的时候（比如火灾、病毒），数据被丢失的可能性很大。我们需要把专业的事情给专业的服务商去做。

既然要有人员来维护服务器，那么就会存在人员信任的问题，在内网系统中一定是“管理员权限大于老板”；在一些公司信息化中，为了节省成本，很多系统被规划到一台服务器中，因此公司不同的技术人员都有可能在服务器上获取数据。技术人员因为不满足公司，而造成彻底毁损数据、泄漏数据、出卖数据的事件不在少数。

3、传统软件系统不能放在互联网上。

很多客户都有分支机构，而且老板有出差或在家中查看公司情况的需求，也就是说存在使用互联网访问系统的需求，如果一个原运行在内网的软件放在公网上，没有 https 加密传输协议和数字安全证书，很难说这样的系统是安全的，这仅仅是局域网系统放在互联网上的众多安全隐患之一。

我们应该相信谁？

随着 SaaS 模式的软件慢慢占领传统软件的市场，新生事物总会受到传统事物的排挤，SaaS 也不例外，就好比爱迪生发明的电灯泡在早期受到蜡烛厂商的排挤一样，不排出一些人站在自己的利益角度攻击 SaaS 的安全性。也不排除一些低劣的 SaaS 的服务厂商中，没有利用更安全的技术，如何辨别具体的一种 SaaS 是否安全，需要把握以下几点：

1、传输协议加密

首先，要看 SaaS 产品提供使用的协议，是 https://还是一般的 http://，别小看这个 s，这表明所有的数据在传输过程中都是加密的。如果不加密，网上可能有很多“嗅探器”软件能够轻松的获得您的数据，甚至是您的用户名和密码；实际上网上很多聊天软件帐号被盗大多数都是遭到“嗅探器”的“招”了。

其次，传输协议加密还要看是否全程加密，即软件的各个部分都是 https:// 协议访问的，有部分软件只做了登录部分，这是远远不够的。目前，Salesforce、XToolsCRM 都是采取全程加密的。

2、服务器安全证书

服务器安全证书是用户识别服务器身份的重要标示，有些不正规的服务厂商并没有使用全球认证的服务器安全证书。用户对服务器安全证书的确认，表示服务器确实是用户访问的服务器，此时可以放心的输入用户名和密码，彻底避免“钓鱼”型网站，大多数银行卡密码泄漏都是被“钓鱼”站钓上的。

3、URL 数据访问安全码技术

对于一般用户来说，复杂的 URL 看起来只是一串没有意义的字符而已。但是对于一些 IT 高手来说，这些字符串中可能隐藏着一些有关于数据访问的秘密，通过修改 URL，很多黑客可以通过诸如 SQL 注入等方式攻入系统，获取用户数据。

4、数据的管理和备份机制

SaaS 服务商的数据备份应该是完善的，用户必须了解自己服务商为您提供了什么样的数据备份机制，一旦出现重大问题，如何恢复数据等。服务商在内部管理上如何保证用户数据不被服务商所泄露，也是需要用户和服务商沟通的。

5、运营服务系统的安全

在评估 SaaS 产品安全度的时侯，最重要的是看公司对于服务器格局的设置，只有这样的格局才是可以信任的，包括：运营服务器与网站服务器分离。

服务器的专用是服务器安全最重要的保证。试想，如果一台服务器安装了 SaaS 系统，但同时又安装了网站系统、邮件系统、论坛系统……，他还能安全吗?在黑客角度来说，越多的系统就意味着越多的漏洞，况且大多数网站使用的网站系统、邮件系统和论坛系统都是在网上能够找到源代码的免费产品，有了源代码，黑客就可以很容易攻入。很多网站被攻入都是因为论坛系统的漏洞。

因此，一个优秀的软件 SaaS 运营商，运营服务器和网站服务器应该完全隔离的，甚至域名也应该分开。

6、重视厂商的历史和专业性，有助于建立信任关系

专业的 SaaS 厂商可能比用户更加注重安全，因为 SaaS 的“安全性”就是厂商的“饭碗”。就像在网上买东西，我们用户需要看看厂商获得用户方面的评价，和媒体的口碑，看看是否专业和专注 SaaS。有些厂商仅仅把 SaaS 产品作为炒作的噱头，可能危害的就是用户。

这样看起来，无论是传统的局域网信息化系统，还是 SaaS 模式的信息化系统，都会让客户关注数据安全。但如果我们有标准来衡量信息化系统的安全性，或者我们提前知晓这些风险的存在，对于用户来说是有利的。

查看原文

化解 SaaS 安全问题的三大措施

在面临云计算应用中的安全性问题时（特别是在软件即服务 SaaS 级别），密码管理不当和不安全协议威胁都将会对您的系统保密造成破坏或数据泄露，同时可能需要由您的企业来承担法律责任。在本文中，我们将探讨 SaaS 所带来的三大威胁，以及能够预先采取措施减轻这些威胁的战略。

本文的目的在于让大家明确，这里所探讨的三大威胁将是您自己能够采取措施而缓解的，而不是要靠供应商来解决。这其中的区别取决于你所使用的"模式"级别（例如 SaaS，平台即服务 PaaS 和基础设施即服务（IaaS）），正如国家标准与技术研究所关于云计算定义中所定义的那样。

请注意，当供应方的威胁仍然可以影响您的服务时，可以进行风险转移，这都是可以通过合同方式进行处理的。

在 SaaS 云服务中最具威胁的因素是什么？

由于 SaaS 模式一般是基于一个瘦型或 Web 客户端，或一组 Web 服务，因此大多数威胁都被留给了供应商。而事实上，供应商处理了几乎所有的威胁问题。这其中对于合同的理解和恰当处理是很重要的。

尽管如此，我的经验表明 SaaS 产品中您必须处理的三大威胁如下：

- 易损证书
- 不安全协议
- 基于 Web 的应用缺陷

易损或不安全的证书

所有有安全需求的云应用都需要用户登录。有许多安全机制可提高访问安全性，比如说通行证或智能卡，而最为常用的方法是可重用的用户名和密码。对于那些缺乏标准管理的证书，密码的强度最小（例如需要的长度和字符集过短），也没有密码管理（过期，历史）。

密码失效是攻击者获得信息的首选方法，而容易被猜到的密码则是主要目标。对于该威胁的最佳缓解措施是：

- 创建一个高强度密码。我建议使用基于短句变形的密码，且至少 8 个字符长。例如，将短句“What a great one for me to know!”变形为“Wagr814me2know!”（注：请不要在实际中使用这个例子）。
- 每 90 天修改一次您的密码。时间长度必须基于数据的敏感程度。
- 不要使用旧密码。

不安全的协议

云应用是远程定义，因此需要基于网络协议功能的通信。但是当供应商配置应用使用不安全的协议时，就可能发生问题。这意味着应用会在客户端和服务器之间使用不具保密性和完整性的协议传递信息。

用户和管理员都经常遇到这类问题。使用不安全协议的应用往往会将使数据暴露给数据传送沿途的任何人，例如远程访问的 Telnet、文件传输的文件传输协议（FTP）、用于邮件的邮局协议（POP）与互联网消息访问协议（IMAP）、以及基于网络访问的超文本传输协议（HTTP）。

为了减轻不安全协议的威胁，您有三种选择：

- 要求供应商替换该协议。例如使用安全壳（SSH）替代用于远程终端访问的 Telnet。
- 要求供应商支持该协议的安全版本。例如，FTP 安全（FTPS），使用 SSL 的 POP，SSL 的 IMAP 和超文本传输协议安全（HTTPS）。
- 使用应用保护连接上的数据。这要求应用在数据上线之前进行加密。注意这是最不可取的选择，因为它涉及核心管理问题。

了解 HTTP

在我们谈及 HTTP 时重要的是要认识到我们并不是要讨论您 HTTP 的起源。使用 HTTP 协议、XML、AJAX 等作为通用封装运送允许应用通过 HTTP 管道传送几乎任何东西。当您听到 HTTP，您可能会想到"网络"。但是在实际中，应用可能甚至会发送您所不了解的数据。

基于网络的应用缺陷

第三大威胁是当客户有能力将适用范围扩大时，也可能引入应用缺陷和安全风险。此类威胁会随具体应用而变化，但也不容忽视。

要成功化解这类威胁，您需要理解您试图扩展的应用。对应用程序编程接口（API）和安全特性进行适当的培训是成功的关键。

接近的想法

我们已解决了公共云 SaaS 产品的三大威胁。管理好您的证书，使用适当协议保护数据和证书，避免引入安全漏洞，将有助于您安全的实施 SaaS 解决方案。

查看原文

（作者：Phil Cox　译者：滕晓龙　来源：TechTarget 中国）

与 SaaS 有关的安全技术

由于 SaaS(Software as a Service 软件作为服务、软件即服务)的出现，软件行业正在经历一场深刻的变革。SaaS 在西方国家已经流行并进入了普及阶段。在中国，虽然近年增长迅速，但大多数企业对 SaaS 这种新的交付模式还缺乏认识. SaaS 的安全技术日新月异，越来越多的企业开始认可 SaaS 安全性和可靠性。

SaaS 的安全从机房开始。机房的安全性包括气体灭火、恒温恒湿、联网电子锁防盗、24 小时专人和录像监控、网络设备带宽冗余、口令进入机房等。服务器和防火墙的负载平衡、数据库集群和网络存贮备份在近几年也成为标准安全性技术。主流 SaaS 运营商多采用双数据中心运营，其中一个机房数据中心为冗余备份。多城市多机房的模式可提高访问速度，但因大大增加安全管理隐患和维护成本，很少被成熟的 SAAS 企业采用。

伴随着 J2EE 和.NET 等基于互联网浏览器软件开发技术的诞生，真正意义上的 SaaS 模式企业管理软件技术起始于 2003 年前后。基于互联网的特点，SaaS 软件有许多区别于前一代软件的独特性，从服务器端软件和数据库、数据传输、到客户端浏览器都出现了许多新技术。.

开发 SaaS 软件系统和开发传统企业应用系统之间有重要区别，标准 SaaS 系统是多重租赁的(Multi-tenant),也就是一套软件和数据库平台，经过软件和数据库的隔离及保密技术，多个企业同时使用。虽然不是多重租赁的 SaaS 产品不一定是“假 SaaS”产品，多重租赁大大提高了运营效率、稳定性，降低运营商的维护和升级成本，变相的说最终消费者得到了价格上的实惠。其他重要的 SaaS 需求，如自定义、SOA 集成接口、离线客户端等，也都会影响 SaaS 应用程序的体系结构。而国外的 Salesforce 的 PaaS(Platform-as-a-Service)和国内八百客公司的 800APP PaaS 代表了 SaaS 的主流架构。

数据库：

SaaS 运营商普遍采用大型商用关系型数据库和集群技术。在数据库的设计上，多重租赁的软件会有三种设计，每个客户公司独享一个数据库 instance，或独享一个数据库 instance 中的一个 schema，或多客户公司以隔离和保密技术原理共享一个数据库 instance 的一个 shema. 几乎所有 SaaS 软件开发商选择后两种方案，也就是说，所有公司共享一个数据库 license,从而降低了成本。

数据库隔离的方式经历了 instance 隔离、schema 隔离、partition 隔离、数据表隔离、到在应用程序的数据逻辑层提供根据共享数据库进行用户数据增删改授权的隔离机制， 从而在不影响安全性的前提下实现效率最大化。

应用程序：

应用程序的安全围绕 Web 服务器展开，比如 Apache、IIS 等。基于这些 Web 服务器，主流厂商多采用 J2EE 或.NET 开发技术并会采用特殊的 Web 服务器或服务器配置以优化安全性并优化访问速度和可靠性。而有些厂商会采用 PHP、Ruby 等开发技术，相比之下，J2EE 和.NET 集成了更多更成熟的安全技术。同样，Oracle、SQL Server 和 DB2 在数据库层面相比 MySQL 等数据库也更加成熟。

身份验证和授权服务是系统安全性的起点，J2EE 和.NET 自带全面的安全服务。J2EE 提供 Servlet Presentation Framework, .NET 提供.NET Framework，并持续升级，因多重租赁带来的整体升级效应使所有使用者共同受益并不需要支付额外的升级费用。应用程序通过调用安全服务的编程接口 (API)，来对用户进行授权和上下文继承。

在应用程序的设计上，安全服务通过维护用户访问列表、应用程序 Session、数据库访问 Session 等进行数据访问控制。并需要建立严格的组织、组、用户树的建立和维护机制。

SaaS 平台是近年来的商业模式热点。一种模式是单一厂商基于 PaaS 应用程序平台提供多种 SaaS 应用，并通过 Web Service 接口提供与其他厂商产品集成。 另一种模式是 SaaS 运营平台，平台厂商提供用户认证，其他软件厂商提供 SaaS 应用程序。在安全性上，PaaS 应用程序平台有着先天的优势。SaaS 运营平台的出现，

为应用程序的开发带来了新的挑战，产品的安全由平台上 SaaS 软件厂商链条中最弱的一个决定，也就是短板效应。

平台安全的核心是用户权限的在各个 SaaS 应用程序中的继承，Salesforce 或八百客等厂商的 PaaS 产品自带成熟的权限树继承技术，自 2006 年以来已经实现大规模商业运营。而第二种运营平台模式类似的集成需要专业的定制开发，相应的中间件技术或 SOA 总线技术还未成熟。

ACL 和密码保护策略也是 SaaS 软件成熟度的标志。客户可在自己系统中修改相关策略。有些厂商还推出了浏览器插件来保护客户登录安全。而在最近半年，国外厂商频繁地开始让用户登录后回答自己预设的秘密保护问题和答案，也是一种为了安全的保护策略，因中国人对这种密码保护策略没有使用习惯，所以在国内还没有广泛的推广开来。

数据传输和客户端：

SaaS 通过互联网而非企业局域网来传输数据和表格。SaaS 和已经普及的网上银行和网银支付都采用 SSL 加密技术，加密位数随着硬件速度的提升而提升。主流厂商通常也会花大笔资金购买专用 SSL 加密设备。八百客、金蝶等国内厂商也提供类似网上银行的 U 盾客户端认证技术。

SaaS 软件都采用浏览器来访问使用，普遍采用的安全技术包括 Cookie 加密、URL 随机码、SQL 等代码的注入防范等技术。当然，浏览器及时升级也非常重要。

成熟 SaaS 厂商也推出了可离线使用的客户端软件。虽然 Salesforce 用“不用软件”的口号吸引了很多关注，但其需要下载安装的离线版也得到了 10%左右的使用率。 而像 RightNow 等其他厂商，在客户端上做了更多的开发和实施工作。八百客的专用客户端还做了呼叫中心、VOIP 电话、短信、电子传真和企业邮局的集成。而这些专用客户端多采用本地数据加密，SSL 传输加密等安全技术。

结语：

不论是 SaaS 软件还是传统软件，企业安全事故多发生于在密码安全管理松懈的企业，虽然 U 盾会在会在很大程度上避免此类安全事故发生。

与网上银行和邮件快递服务类似，优秀 SaaS 服务商承诺的安全和可靠性也将被更多企业用户接受。 安全是一个优秀 SaaS 厂商的长期承诺。

查看原文

（来源：TechTarget 中国论坛）

告别“纸上谈兵” 如何建立安全的 SaaS 服务

据市场研究公司 IDC 预测，随着云计算模式的流行，未来几年 SaaS 应用将增长迅猛。到 2012 年，85%的新型 IT 服务供应商将专注于 SaaS 服务。

来自 Gartner 的调查研究也表明，与上一年相比，企业 IT 用于 SaaS 的开支今年增加了 14%。这个结果的大部分原因是企业越来越多地把他们的软件和基础设施转移到云上。

毫无疑问，无论是 SaaS 服务商队伍规模的扩大还是应用 SaaS 企业数量的增加，都表明软件即服务（SaaS）的市场正在蓬勃发展。另外，Salesforce、Google、八百客这些云时代“明星”的兴起，更为云服务和云软件的发展起到很大的推动作用。

近两年，SaaS 已不再是概念性的“纸上谈兵”——技术的成熟、业内看好后的投入，都使得 SaaS 在形势上表现得“山雨欲来”。特别是一场金融危机迫使企业加强“内功”建设， IT 投资慎之又慎。通过租赁的方式享受软件服务，对许多企业来说是应用先进技术的最好途径。它不仅降低了企业的软件服务成本，缩短了信息化建设周期，还大大减少了企业的运维成本。这样，SaaS 的需求就平添了些许“刚性”成份。

基于上述诸多成熟的条件，SaaS 开始了前进的过程，但是，SaaS 要想告别“纸上谈兵”时代，真正进入企业并被全心接受，还差最后短暂却充满荆棘的一步——建立信任。

提高安全性带来信任

SaaS 遭到用户质疑是很正常的，新技术带动新的 IT 业务模式的诞生、发展，无不伴随质疑。电子商务的例证可以说明 SaaS 被人们认可的趋势毋庸赘言，但不能忽略的是观念改变的时间序列。谁都不能否认 SaaS 被认可需要时间。而且，时间对观念改变的作用仅局限于必要条件，就是说“静等”是决定性的。努力改善 SaaS 自身的安全性，才是 SaaS 被认可的充分条件。SaaS 供应商在完善所应用的技术时，需要投入大量努力保证安全性。

1、数据的安全

SaaS 的应用，用户需要将数据托管给服务商，而且是异地存储，对于一些数据敏感性分类较差的企业，其往往是全部数据集中存放，此外，SaaS 供应商难于分辨敏感性等级，加之其自身存在程序漏洞或特权用户泄漏的可能性，这都对数据安全构成威胁。

针对这一问题，所有数据，包括有管理权限的访问，都应该被记录下来，并定期审计。SaaS 的应用体系结构和数据模型的设计应确保正确的数据隔离。应该使用强大的密码保护，以确保在数据访问上的安全控制。

作为国内最专业的 SaaS 厂商八百客，数据的机密性、完整性和可用性是客户与八百客共同成功的命脉。八百客 URL 访问数据安全技术和搜索引擎隔离技术，有效的防止没有权限客户通过 URL 注入方式获取非法信息，防止搜索引擎等机器人非法扫描本系统，使客户的数据安全性大大提高。

2、SaaS 应用程序的安全

SaaS 解决方案所部署的环境往往是公共云，在开放的公共云部署首先确保其安全性。特别是采用托管 SaaS 的部署要求提供方提供相关服务(防火墙，入侵检测系统等)来强化其安全性。

目前解决方案是利用安全审计可以更好地识别任何安全问题或威胁，以确保您的企业数据的安全。定期进行应用和网络性能评估。这些有助于验证 SaaS 应用和部署的安全性和完整性。

3、网络安全

网络的安全是个长期的话题，企业和 SaaS 提供商之间的数据流，往往构架在公共网络，在传输过程中无处不在的攻击、窃取敏感信息。

中小企业基本上依赖 SaaS 的供应商应用诸如 SSL 确保数据在互联网上流动的安全性，或者在 SaaS 的部署网络中采取加密技术，防止网络渗透、拒绝服务(DoS)。

4、业务连续可用的安全

企业的应用需要支持高可用性，以确保其能够 24*7 地业务连续。SaaS 模式的架构设计和基础设施，能否适应硬件/软件故障以及拒绝服务攻击成为关键问题，以确保停机时间最短。

目前解决方案是 SaaS 企业所提供的安全备份和恢复服务，即强化基础设施建设和云级恢复服务的能力，这都是要促进灾后恢复和减轻对敏感数据的丢失。而且备份的数据应该得到严格保护，如业务数据等就需要使用强大的加密机制。这些检查也是非常必要的，它可以减少未经授权的访问和敏感数据泄漏的风险。

综上，SaaS 供应商安全措施总体原则：采用完善、成熟的网络架构，严格的安全设计，对网络、关键应用采取了多级容灾、冗余方案。

树立品牌加强信任

目前国内还没有在 SaaS 方面取得巨大成绩的 SaaS 服务商，对于管理者来说，他们往往会有这样的顾虑：“服务商会不会比我先死？”虽然他们确实认识到了 SaaS 的优点，有意寻找合作伙伴，但对服务商能否跟自己一起发展壮大仍然保持怀疑的态度。信息的不对等让服务商和广大中小企业在双向选择中感到束手束脚。

解决这个问题要从多方面出发，但从服务商方面来说，要力求稳扎稳打，树立“领先品牌”的品牌形象，建立清晰的企业形象识别系统，加强企业的信任度，用产品和服务赢得用户，同时壮大自身的实力。资金有限的服务商选择项目应该首先从用户的角度出发，把每一分钱都用在刀刃上，千万不能盲目自信，浪费资源。

提升服务巩固信任

服务是 SaaS 的关键，也是重点。服务的好坏决定了 SaaS 能否取得用户的认可，能否持续发展下去。因此，提升 SaaS 服务质量，提高用户对服务的满意度至关重要。

服务级别协议(SLA——Service-Level Agreement)是我们通常用来判断一个 SaaS 服务是否令用户满意的工具，SLA 是一项针对提供某种程度上的稳定性的厂商的合同义务，目前使用 SLA 协议的用户达到了 99%以上。SLA 的保障是以一系列的服务水平目标(SLO)的形式定义的。服务水平目标是一个或多个有限定的服务组件的测量的组合，SLO 被实现是指那些有限定的组件的测量值在限定范围里。总之，

任何一种服务的满意程度都可测量出来，即使不能完全定量化的反应，也可模糊的定性，甚至是否决。

此外，SLA 协议还包括如果合同到期的话，SaaS 服务提供商应该如何处理用户数据的条款，在这种情况下，用户应该确保拥有这些信息的所有权，并且确认是受到法律保护的。这点就成为 SaaS 能否延续被更广泛在中小企业中应用的法律前提，法律又是对服务满意度诠释的保证。SaaS 模式只有在法律的合规性层面上没有了瑕疵，中小企业对它才能完全信任。

SaaS 模式已成为软件业发展的主流趋势。只要 SaaS 的品质和可信度能继续得到证实，它的魅力就不会消退。建立信任——这一较“软”性的竞争力因素，决定着 SaaS 模式软件生存、发展的空间，也是 SaaS 真正告别“纸上谈兵”时代的关键一步。

查看原文

SaaS 安全与应用探讨

SaaS 模式的产生给传统软件行业带来了巨大的冲击。它改变了传统软件的交付方式，让更多的用户共享强大的计算应用与存储功能，并把用户从软件运行维护、升级等一系列复杂操作中解脱出来。但是如此灵活的数据访问方式与高度的共享性会不会给数据安全保障带来毁灭性的灾难呢？SaaS 又如何来满足离线用户的应用呢？

在周四举行的第四届中国软件运营服务（SaaS）大会上，百会市场总监余凯就 SaaS 的安全与应用问题接受了 TechTarget 中国记者的专访。

如何应对 SaaS 的安全问题？

在概括 SaaS 应用的安全现状时，他表示：“目前市场方面，SaaS 产品的安全问题是用户普遍关注的焦点。”随后，在探讨如何应对 SaaS 的安全问题时，他说：“安全的保障其实可以从两个方面来着手，一方面要看供应商提供的安全措施和管理机制是不是可以保障用户数据不丢失，此外，做到不窃取用户数据；另一方面是供应商的品牌是不是足够支撑起这块业务的信誉问题。”

离线状态下如何实现 SaaS 模式？

SaaS 模式将很多操作都转变为在线方式，那离开了互联网，SaaS 模式如何实现？余凯进一步阐述了离线状态下的应用场景，他表示供应商提供强大的离线服务显得非常必要，支持用户离线备份，离线下载。他也强调：“随着科技的发展，未来大家处在离线状况的机会是非常少的。此外，加入到互联网的用户端会越来越多，未来每个人都能随时处于在线状态。你的计算机不在线，但是你的手机，你的电视机可能是在线的。特别是实现物联网与三网融合之后，随时在线会变得更加容易。”

由此，我们可以看出，虽然 SaaS 安全机制是目前一个比较棘手的问题，但仍是有章可循的。此外，随着用户端与在线方式的增多，SaaS 将会更加贴近用户。

查看原文

（作者：王涛　来源：TechTarget 中国）