bsi.

...making excellence a habit.™

ISO/IEC 27018

云隐私保护

白皮书

摘要

隐私信息安全从未受到如此高度的关注，包括国际标准化组织(ISO)、美国政府以及欧盟在内的许多国家、地区和组织都在采取各种措施来应对隐私信息安全问题。这些机构达成共识的原因，则是国际标准ISO/IEC 27018。

数据泄露的规模[1]

3,046,456
- 每日

2,116
- 每分钟

126,936
- 每小时

35
- 每秒

ISO/IEC 27018是公有云服务中个人可识别信息保护的一种行为准则。它在体系结构上沿用了被广泛使用且备受重视的ISO/IEC 27002信息安全控制行为准则的框架。那么，ISO/IEC 27018能够为客户提供什么？它又为何如此重要？

个人数据泄露的潜在风险已成为国际首要议程。大量重大信息安全事件已将人们的注意力引向如何保护自己的个人详细信息。如果审视一系列安全事件以及受影响的人员的数量，您就会清晰了解这一问题的严重程度：涉及超过2100万名政府雇员的美国人事管理局(US Office of Personnel Management)的数据被窃取；针对英国电信运营商维尔豪思(Carphone Warehouse)的攻击使其200多万客户受到影响。这些只是2015年一个季度所发生攻击事件的冰山一角。实际上根据泄露等级指数（Breach Level Index,BLI）统计，2015年 7.075亿数据被泄露[1]。

而企业对安全的投入比以往更多。根据IDC的统计，到2020年，全球IT安全支出达到1.016亿美元[2] 。

许多人已经深谙黑客与社会格格不入的形象；大部分源自外部的攻击均是由组织有序的犯罪团伙或国家资助的机构所操纵，要采取措施应对此类威胁极其困难。另一个更大的潜在风险是企业内部人员蓄意或无意地为攻击“敞开大门”。

内部威胁相比之下更加危险，因其往往未被报道或被刻意掩饰。根据普华永道(PricewaterhouseCooper)的研究[3]，75%遭受因员工所导致的安全攻击的企业既未被执法，也未受到法律指控。这意味着，此类企业的客户面临遭受攻击的风险，任何在未来雇佣此类人员的公司可能无从知晓其以往的所作所为，从而可能为未来攻击留下可乘之机。

2016年上半年就出现64%已识别的数据泄露盗窃，致使保护个人数据令人如此不安，这也丝毫不足为奇怪，特别是，人们为何对云如此恐惧却对于委托云服务供应商管理数据一直保持着沉默？

正是出于这些原因，欧盟已实施关于数据保护的新法规，试图在整个欧洲大陆协调法律状况。在欧洲，有各种各国特定的数据保护法，这使得云服务供应商的运营极其困难。云可以跨越国际界限，而各个国家的数据安全管理法规却存在差异。

[1] http://breachlevelindex.com
[2] http://www.computing.co.uk/ctg/news/2474455/global-it-security-spending-to-top-usd100bn-by-2020
[3] http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

企业和云服务供应商拥有和管理数据的方式也是问题的一部分—存在法律分责的情况。它们代表其客户管理数据，而客户则对此类数据所发生的情况承担着法律责任。

企业真正担忧的焦点在于：所有云服务供应商都乐于谈及其安全专业知识、对于数据保护的投入力度以及设置的防范数据威胁的“屏障”，但潜在焦虑是云服务供应商是否与客户采取相同的方式来对待机密数据。

于数据保护领域，欧盟正在引入一致性，而美国的状况则不同。

一些国家缺乏监管个人数据使用方式的国家法规。各个国家的不同政策还可能导致一定程度的混淆。不同行业的不同法规需求又加剧了这种混淆。所有这些因素相结合促使制定一致的数据保护政策绝非易事。

为了解决这一问题，美国国家标准技术研究院 (National Institute of Standards Technology, NIST) 于2015年8月建议联邦机构“在其任务和决策活动中使用有效和适用的网络安全国际标准”[4]。随着美国政府机构实施这些标准，它们将要求其承包商和供应链也符合各种标准的要求。

ISO/IEC 27000

从国际角度看，ISO开发了一系列信息安全标准，为企业提供框架以开发流程和程序来解决整个企业的信息安全问题。

在这一系列标准中，首要的是ISO/IEC 27001，这是获得最广泛认可的标准，旨在防止敏感信息无意分发和未经授权的访问。

借助其114项控制，ISO/IEC 27001及与之十分密切的ISO/IEC 27002能够缓解信息采集、存储和传播所涉及的风险：

- 提供要求以实施有效的信息安全管理体系
- 允许组织遵守政府增加的法规及行业规定的特别要求
- 让企业在发展的同时了解其所有机密信息始终处于保密状态

[4] http://csrc.nist.gov/publications/drafts/nistir-8074/nistir_8074_vol1_draft_report.pdf

ISO/IEC 27018标准

ISO/IEC 27001一直沿用至今。为了处理云计算技术所引发的问题，ISO于2014年秋季创立了一项新的标准—ISO/IEC 27018。云服务供应商要采用这一标准以确保客户数据安全，让客户能够安枕无忧。这一新标准是对ISO/IEC 27001和ISO/IEC 27002标准的扩展，为云服务供应商如何处理个人可识别信息(PII)的企业提供了指南。对于企业而言，这有点像法律“雷区”，原因之一在于《欧盟一般数据保护条例》(EU GDPR)经过长时间才予以通过，不过，首先需要做的是明确一些法律定义。最关键的定义是PII本身，这是所有讨论的基础。

PII被定义为(a)可被用于识别与此类信息相关的PII当事人，或者(b)可直接或间接与PII当事人关联的任何信息。

当然，这引发了另一个问题—如何定义PII当事人？这一问题更复杂，因为在一些国家，这一实体指的是数据主体。同样，对于PII控制者（有时称为数据控制者）的定义也存在一些模糊性，不过，核心的一点在于PII控制者是数据处理目的的确定者。

ISO/IEC 27018包含什么？

这一标准包含若干指南，根据ISO定义，这些指南旨在：

- 帮助公有云服务供应商在作为 PII处理者开展业务时承担必要的责任，无论此类责任是否直接或通过合同明确应
- 使公有云PII处理者在相关事务中保持透明，从而让客户可以选择经过良好治理的，基于云的PII 处理服务
- 协助客户和公有云PII处理者达成合同协议
- 为云服务客户提供行使审核和合规权利及责任的机制。单独的—个人云服务客户审核托管在多方虚拟化服务器（云）环境中的数据可能在技术上不切实际，同时可能增大物理及逻辑的网络安全风险

尽管这些只是一些尚待完善的原则，但如果审视这些原则的含义以及它们能够如何为客户提供帮助，我们就可看到，第一次有了针对个人数据处理的真正框架。

ISO / IEC 27018将ISO/IEC 27002中描述的一系列安全控制作为基础，然后以两种方式扩展。首先，在许多领域中扩展了现有的安全控制，以处理云服务客户和云服务供应商之间的责任。其次，添加了一组新的安全控制，以反映ISO/IEC 29100隐私框架标准中定义的隐私原则。

扩展的安全控制包括如下:

- 在存储和任何可移动的物理介质中，对PII进行加密的要求
- 一旦数据不再需要，在指定的时间内删除PII
- 符合云服务协议中明文规定的目的时，才进行PII处理
- 如法规所明文规定，在处理PII原则的权利问题上，可检查和纠正PII

ISO/IEC 27018能够确保云服务供应商在处理PII方面有着适当的程序。它还可以帮助制定更强的云服务协议。该标准就PII的问题，规定了CSPs如何培训员工，需要什么文件程序，并提供了相应的指导方针。

ISO /IEC 27018旨在为云服务客户提供真正的透明度，以便客户能够清楚了解云服务供应商商在保护和保护个人数据方面所做的事情。

在实施这一标准时，企业须考虑到下列三个方面：

- 是否有企业必须遵守的现有法律和法规要求，包括任何行业特定规则和法规
- 遵守ISO/IEC 27018是否会为企业招致更多风险
- 采用此标准是否会与企业的政策和企业文化背道而驰

结论

对于云计算行业需要标准化来提供充分而有效的信息安全是毫无疑问的。根据TrustE在2015年的一项调查，92%的英国网络用户担心其个人隐私。最大的问题是用户不知道他们在网上收集的个人信息是如何被使用的，以及公司分享个人信息的可能性。越来越多的消费者要求企业在采集、使用和保护其线上数据方面能够变得更加透明。

ISO/IEC 27018有助于将行业的关注焦点集中于提供更大的安全性，从而有效保护PII。这一标准已经获得一些主要的云服务供应商的支持：Microsoft Azure, IBM Softlayer, Google Apps for Work, 亚马逊网络服务以及 Dropbox 均已获得ISO/IEC 27018认证。预计更多云服务供应商将紧随其后，越来越多的企业将把更多的信息移至云端，以获得更大的技术灵活性和资源需求降低所带来的优势。不过，随着云技术被更广泛应用，安全（尤其是隐私）问题不容忽视。

欧洲法规的实施将确保隐私保护所采用的新方式成为当今的新秩序。

ISO/IEC 27018为客户和云服务供应商等提供了一套针对PII适当保护的指导方针。

它不是国家和国际法规的替代，广泛采用这一标准也不意味着服务供应商自动遵循了相关法规要求，但是，它将成为发展道路中的重要一步。

了解更多
有关BSI解决方案
能够帮助您的企业
有效保护数据信息，
请访问：bsigroup.com

为什么选择BSI？

自1995年以来，BSI便始终处在信息安全标准的前沿位置。ISO/IEC 27001——世界上应用范围最广泛的信息安全标准，最初是由BSI制定颁布的BS 7799转化而来。我们从未停止脚步，如今我们仍致力于新问题（如网络与云安全）的解决方案。这就是为何我们是最具资格帮助您理解标准的原因所在。

BSI致力于通过标准助力客户的成功，进而实现卓越。我们帮助组织将韧性融入业务运营，帮助其实现可持续发展，适应变化并保持长期繁荣。我们让追求卓越成为习惯。

一个多世纪以来，我们的专家一直向平庸和自满发起挑战，旨在将卓越变成一种习惯融入人员和产品中。BSI在全球182个国家/地区拥有超过80000家客户，其标准在全球成为实现卓越的“助推器”。

我们的产品和服务

我们为您提供独特的产品和服务互补组合，这些产品和服务通过我们的三大业务流（知识、认证和合规）进行管理。

知识

我们业务的核心在于所创建并传授给我们客户的知识。在标准领域，我们不断强化我们作为专业机构的信誉，汇集来自行业专家的集体智慧打造本地、区域和国际不同层次的标准。全球十大管理体系标准，其中八个是由BSI制定颁布的BS标准转化而来。

认证

根据特定标准对流程和产品符合性的独立评估可确保我们的客户能够实现高水平的卓越性。我们会就世界级的实施和审核技巧对我们的客户进行培训，以确保他们能够最大限度发挥标准的优势。

合规

要获得实实在在的长期优势，我们的客户需要确保持续合规，满足市场需求或标准，并让合规成为一种植入组织的习惯。我们提供管理咨询服务和具备差别化优势的管理工具来促进这一流程。

要了解更多信息

www.bsigroup.com
400 005 0046
infochina@bsigroup.com

关注bsi微信