atsec 新闻简报

atsec(Beijing) information technology Co., Ltd

Room 119, Building 2, No.1, Street 7, Shangdi,

Haidian District, Beijing, P.R.China 10085
Tel +86-10-84834011
Fax +86-10-82890017

www.atsec.com

atsec NEWS 04/2012
the information security provider

众人拾柴火焰高，共筑支付安全

atsec，白海蔚

PCI DSS 背景和现状

自 2006 年美国运通（American Express）、美国发现金融服务（Discover Financial Services）、JCB、万事达（MasterCard Worldwide）和 Visa 国际组织五家支付品牌共同筹办设立统一且专业的支付卡产业安全标准委员会（PCI SSC: Payment card industry Security Standards Council）以来，整个支付产业链上的不同机构(发卡机构、商户、收单机构、服务提供商等)给予数据安全保护很大的重视。以我国为例，越来越多的网络商户和第三方支付服务提供商完成了 PCI DSS 数据安全标准的合规认证，且越来越多的银行开始致力于 PCI DSS 标准的合规建设。在 Visa、万事达等卡组织以及多方的努力和大力推动下，通过 PCI DSS 数据安全标准的合规认证来进行数据保护，对保护持卡人利益的重要性方面有了更高的提升。

截至目前，国内已完成 PCI DSS 数据安全标准合规建设的机构包括但不限于：快钱（99bill）、易宝支付（Yeepay）、Oncard Payments、首信易（PayEase）、盛付通、票务在线、安利（中国）等等。此外，诸多大型商业银行也已经启动并完成了 PCI DSS 的部分合规建设工作。

与此同时，atsec 作为 PCI 授权认可的第三方安全审核机构 QSA 和脆弱性扫描服务商 ASV，为了给中国的客户提供更加便捷且专业的服务。于 2011 年 8 月，atsec 中国在已往 atsec 全球品牌拥有 PCI QSA 和 ASV 资质的基础上，进一步以单独的实体正式向 PCI 安全标准委员会递交 QSA 和 ASV 资质申请，由此成为中国首家也是唯一一家在 PCI 安全标准委员会授权列表中的本土企业。在申请资质的过程中，标委会全面审核确认 atsec 中国的管理体系及审核方法论，严格考核团队每一位审核人员的信息安全经验和专业知识，评估提交的报告等证明。经过不同层面的审批，atsec 中国团队获得 PCI 安全标准委员会的进一步认可，并称赞 atsec 中国高效、严谨的工作风格，相信这是一个新的里程碑，将为我们中国的客户在执行 PCI DSS 合规建设的项目中提升更多的信心。atsec 中国团队将一如继往的为支付产业链信息安全工作做出贡献！PCI DSS 授权资质链接如下：
https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

为支付安全添砖加瓦

俗话说众人拾柴火焰高，正如支付产业链上环环相扣的数据保护一样。从数年前支付网关类公司最先执行 PCI DSS 标准合规，到陆续大型商户、收单银行等不同角色致力于标准的合规建设工作,PCI DSS 数据安全标准从交易流程着手，搭建并确定合理、有效的持卡人数据环境，从每个环节执行严谨和高安全性的保护措施，使得整个支付产业链安全、稳定地发展。

最近新闻一览

更多的新闻，请参见我们的网站：
www.atsec.com

正如民生银行信用卡中心高海涛先生所述：

“随着网络经济和电子商务的兴起，网上消费已经成为了一种时尚和潮流。但是这种便捷的消费模式背后，却蕴藏着很大的交易风险和安全隐患。在整个支付卡产业链条中，无论是收单商户还是发卡银行，任何一个环节处理不好，轻则泄露客户隐私，重则影响客户的资金安全。近年来，随着第三方支付和其他一些新兴支付手段的出现，更是将这种风险快速放大。在这种背景下，如何保障持卡人的数据安全，就显得尤为重要。

持卡人的数据安全需要支付卡行业各参与方的整体提升，这就要求每个支付卡行业的参与主体，包括发卡银行、收单机构以及商户的共同努力。那么如何才能快速提升整个行业的信息安全管理水平，我觉得提高技术准入标准就是一个很好的抓手，由于国内的支付卡行业起步较晚，这方面的技术标准和规范还十分欠缺，而国外的支付卡行业已经经历了几十年的发展，积累了大量的经验和最佳实践，借鉴国外成熟的做法和经验无疑是推动整个行业快速成长的一条捷径。

PCI-DSS 是 VISA、MasterCard 等国际卡组织参与制订的专门针对支付卡行业数据安全的技术标准，该标准适用于支付卡产业链条中的所有参与主体，包括发卡机构、收单机构以及商户，国内外大量的实践证明，通过实施 PCI-DSS 合规项目，可以有效提升企业的信息安全管理水平，增强客户的信任度和品牌影响力。

民生银行信用卡中心历来十分重视持卡人的信息安全保护，目前我中心正在以收单系统为试点实施 PCI-DSS 合规项目，在 atsec 咨询团队的帮助下，项目正在有序推进。通过实施该项目，我中心人员的安全意识得到了明显的提升，技术措施和管理手段也得到了进一步的完善。该项目实施完成后，我们有信心为民生银行的信用卡持卡人提供一个更加安全的用卡环境，同时也借此机会，向 atsec 的民生服务团队表示感谢，在项目实施过程中，你们表现出了强烈的服务意识，严谨的工作态度和专业的技术素养。谢谢你们为民生银行信用卡中心信息安全工作做出的努力和贡献！”

atsec 作为 PCI 安全标准委员会授权认可的第三方审核机构，倡议支付产业链上的不同角色加入到标准委员会的参与机构当中，将自身企业在采用 PCI DSS 标准进行合规建设的经验和心得共同分享。参与机构包括协会组织或商业机构、金融机构、各类商户、POS 厂商、支付处理机构和其他机构。截至目前，已有参与机构达 640 家，可在如下列表查看：https://www.pcisecuritystandards.org/get_involved/member_list.php

在以往的审核中，atsec 与支付产业链上不同角色机构合作执行 PCI DSS 的合规建设。针对已经完成 PCI DSS 合规建设并持续合规的机构，直接参与合规建设的项目管理者或者执行者也纷纷提出了他们的感言：

- 安全、信赖是电子支付日渐走入大众生活的根本，同样支付服务方也应以资金安全、信息安全为提供服务的根本和基础。快钱率先通过 PCI DSS 最新版本的审核认证是权威组织对于快钱的肯定，同时也宣告快钱拥有国际领先的安全支付系统及信息安全解决方案。另外，关国光表示，支付企业积极参与 PCI 认证审核也有助于中国的支付行业更规范、专业。 ——快钱 CEO 关国光
- 安全、可靠’是电子支付平台能够持续健康发展的基础，易宝支付早在 2007 年 3 月，就率先作为独立支付公司通过了国家信息安全测评中心的安全认证，此次再顺利通过 PCI DSS 合规性评估，意味着易宝支付的交易平台整体安全水平、风险控制体系已达到了一个新的高度。 ——易宝支付 CEO 唐彬
- BilltoBill 作为在中国领先的信用卡支付公司，在风险控制，防伪反欺诈以及系统的数据安全方面有着优良的记录。这次选择 atsec 是因为他们的资质，良好的反应速度以及专业的项目管理；通过本次 PCI 认证的合作，能够更好的增强 BilltoBill 支付系统的安全性，保护持卡人的数据安全。 ——原 BilltoBill CEO 雷扬
- 作为电子商务行业，大麦网始终坚持确保客户机密信息的安全和完整，此次与 atsec 团队携手，采用国际安全标准，完善并巩固了大麦网的安全架构和内部风险控制系统。我们感谢 atsec 的努力，期待进一步的合作。 ——大麦网董事长曹杰

- PCI DSS 作为全球最严格的数据安全标准，我们能够顺利通过该认证，说明盛付通支付系统的安全性方面已经达到了国际要求，这也意味着用户在享受盛付通服务的时候，拥有了国际水准的安全保证。 ——盛付通首席执行官王静颖

- PCI DSS 的标准要求既具体又严格，尽管安利中国早已在信息安全领域通过了 ISO/IEC 27001 认证，但针对此次的台湾 POS 系统的 PCI DSS 合规建设项目，整个项目组仍然遇到不少技术层面的挑战。在项目过程中，atsec 顾问不仅认真细致地完成了差距分析和最终评估等各项工作，更难能可贵的是，他们凭借着在 PCI 领域的专业知识和丰富经验，为我们提供了很多有价值的意见和建议，使所有的技术难关得以攻克，并最终顺利实现 PCI DSS 合规。此次 PCI DSS 合规的实现，标志着安利中国为台湾 POS 系统的支付卡信息安全保护达到了国际标准的要求，意义重大。我们非常感谢 atsec 的指导和帮助，并期待与之进一步的合作。 ——安利中国沈国华

- PCI DSS 可以帮助我们证明公司对于持卡人信息的相关安全保障满足行业性的安全标准要求，从而加强客户对于我们确保客户相关信息处理过程中的信息安全信心。——快钱刘锦祥

- 安全、信赖、可靠是电子支付平台能够持续健康发展的基础，盛付通此次顺利通过 PCI DSS 合规性评估，意味着盛付通的交易平台整体安全水平、风险控制体系已达到了一个新的高度。在此过程中，atsec 对盛付通进行外部渗透测试，以确定是否存在可能成为恶意攻击入口点的网络漏洞以及可被利用的安全性缺陷，并为盛付通提供了专业的工具和技术支持，以帮助我们更好地确保在支付处理环节中信用卡数据等机密信息的安全。——盛付通叶飞

- PCI DSS 合规评估对于支付公司来说，不管是监管要求、合作门槛，还是用户对品牌的安全体验，都具有重要意义。我司在五个月内能完成 PCI DSS 合规评估，和 atsec 团队高效、务实的工作是分不开的。项目中，我们也都感受到其认真、细致、严谨的工作态度和熟练扎实的专业技能。非常感谢 atsec 团队为我们安全体系建设做出的贡献，期待与 atsec 安全专家的再次合作！——盛付通杜磊

- 众所周知 PCI DSS 认证过程异常严格且复杂，必须通过自我安全检查、漏洞分析以及由协会执行的安全调查这三个步骤，审查范围包括了硬件、软件、工作流程、员工、用户等诸多内容，总共有 200 多项审查项目。在盛付通 PCI DSS 认证过程中，很好的体会到了 atsec 团队中咨询师自身扎实的专业技能，严谨认真的工作态度。在评估后期，由于项目时间紧，且接连出现了多个未预料的问题，atsec 的高向东先生在连续加班工作近 1 个月后，出现头痛发烧，仅是休息了一个下午，第二天又继续加班工作，我们能够顺利在计划内通过 PCI DSS 认证，高向东先生功不可没啊。感谢高向东先生，他在负责 PCI DSS 认证的相关制度文档审核工作，他是一个非常专业且严谨细心的人，帮我们标出了文档中不恰当的地方，并且给出了详细的修改意见，减少了我们文档的修改次数。——盛付通黄永飞

- 只有支付产业链上每一个角色包括银行、第三方支付公司以及所有的商户都做到数据安全的合规建设，让每一个环节都提高信息安全的意识，才能保障整个支付产业链的数据安全。工商银行作为世界 500 强企业，一直以来注重信息安全的保护，不论在技术手段还是管理流程上都力求做到最好。PCI DSS 合规建设项目目前正在紧锣密鼓的开展中。项目实施过程中，随着对 PCI DSS 标准的理解更加深入，让我们体会到该标准的全面性和严谨性，以及对技术的高要求。我们有信心在依照 PCI DSS 标准进行合规建设后我们的持卡人数据环境将更加健壮，将使得工商银行为客户提供更优质且有保障的服务。atsec 团队与我们并肩作战，紧密配合我们按照预期计划顺利的开展各项工作。我们感谢 atsec 给予我们的高度配合，期待我们的 PCI 认证项目圆满完成！——工商银行 黄汉波

不难看出，不论是已经完成了 PCI DSS 标准合规，还是正在致力于合规建设，获得 PCI DSS 合规认证的成功都需要各方的重视和大力的配合，而该合规的结果让企业自身具备了更完善、更规范的管理体系，拥有了相对健康、安全的网络环境，而对于持卡人来说享受安全、便捷的交易方式无疑提升了对公司的知名度和信任度的认可。在全民进入卡生活时代的今天，保护持卡人的信息，筑建支付产业链的安全需要我们大家共同的努力！

水涨船高，我眼中的外部安全扫描

atsec 王长龙，陈谨运

2011 年已经成为历史，但是在 2011 年中发生的安全事件对于大大小小的企业或许至今仍然历历在目。索尼 PSN 入侵事件，CSDN 信息泄露，韩国著名游戏公司 Nexon 遭黑，花旗银行网站遭遇黑客等事件可以说在引起众人广泛关注的同时也警示我们：企业对外提供服务的安全性对于企业来说尤为重要。

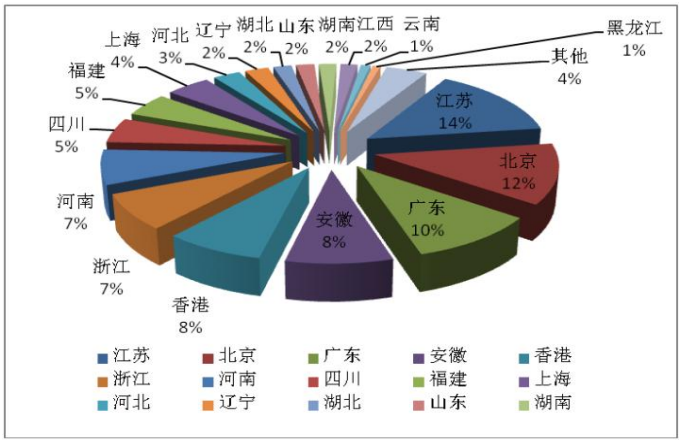
在开始进入正式讨论之前，我们先看两组由中国国家信息安全漏洞库（CNNVD）发布的 2012 年 03 月 05 日至 2012 年 03 月 11 日一周的安全统计数据。第一个图表是对于上述日期内被发现漏洞的类型统计：

序号	漏洞类型	漏洞数量	所占比例
1	输入验证	18	20.69%
2	资源管理错误	14	16.09%
3	SQL 注入	10	11.49%
4	跨站脚本	10	11.49%
5	缓冲区溢出	7	8.05%
6	权限许可和访问控制	5	5.75%
7	设计错误	3	3.45%
8	路径遍历	2	2.30%
9	信息泄露	2	2.30%
10	代码注入	1	1.15%
11	跨站请求伪造	1	1.15%
12	授权问题	1	1.15%
13	其他	13	14.94%

图表 1：漏洞类型统计表

从上述漏洞类型统计分布情况看来，绝大部漏洞都能够轻易的被恶意人员通过企业外部执行攻击活动如输入验证、资源管理错误、SQL 注入、跨站脚本、缓冲区溢出、权限许可和访问控制、路径遍历、代码注入、信息泄露、跨站请求伪造等等。

第二个图表是2012年03月05日至2012年03月11 日一周期间，CNNVD抽样监测我国大陆地区网站被挂马的统计示意图。在一周之内，CNNVD发现2830个网站被恶意入侵并被安装了木马，以下是被挂马网站按地区分布的情况。



图表 2：被挂马网站按地区分布图

从信息安全的角度看来，上述简单的两组数据能够很直观的反映出当前大部分企业对外提供服务的基础设施存在很多的安全隐患并且也可能会为企业带来很大的安全风险。

随着计算机技术的普及，黑客的攻击越来越频繁，攻击手段越来越高深且多元化。互联网的广泛发展，资讯变的更加发达，更多的人很容易就能获得漏洞的信息以及知晓该漏洞的攻击方式，也就意味着企业对外提供服务的基础设施所遭受的安全风险在日益的增大。如何能够把公司或者企业对外提供服务的安全级别提高从而降低对外提供服务被入侵的可能性将是我们这篇文章需要探讨的话题。

通过atsec对信息安全领域专业知识的理解以及长达十余年的安全实践经验，我们认为定期为企业对外提供服务的基础设施进行安全扫描或者安全评估，并根据评估结果进行切实整改能够有效的降低企业来自外部的安全风险。

外部安全扫描（业界也就漏洞扫描）起始于 90 年代，它是基于互联网的远程脆弱性评估的活动。这项工作主要是由具有安全知识的人员通过操作安全扫描工具来完成，扫描工具根据内置的扫描插件去判断和确定被扫描目标机器上是否存在某些已经被披露的安全漏洞，并针对安全漏洞给出相应的解决。安全扫描适用于任何基于互联网对外提供服务（如 WEB 网站，电子银行，门户网站，论坛等），对外提供服务的服务器诸如 FTP 服务器、数据库服务器，网络设备等的公司或者企业。

通过安全扫描，企业能够全面的评估系统（外购的第三方产品）在技术层面存在的安全脆弱性并了解当前所面临的安全风险。通过对脆弱性进行整改或者制定相应的控制措施，企业能够有效的降低对外提供服务的基础设施所面临的安全风险；通过安全扫描，企业能够识别出自身开发产品（如WEB应用程序）存在的安全脆弱性，并可根据扫描结果提出的建议有针对性的对某个领域的安全编码进行加强和完善。

安全扫描主要的目的是通过自动化的方式在技术层面查找某些已经被发现和公布的脆弱性，或者某种特定类型的脆弱性。这项安全工作对于很多公司解决自身的安全问题而言可能并不足够，因为我们知道安全风险不仅仅来源有技术层面的实现，它还可能存在我们的人员的安全意识，日常操作以及企业的管理流程当中。对于这种类型的企业我们建议可以参考一个目前在国内、外都备受关注的关注在整体环境安全建设的标准：支付产业数据安全标准（Payment Card Industry Data Security Standard 简称PCI DSS）。

该标准建立的初衷是为了保护持卡人数据，所以该标准要求无论在规章制度，操作流程，人员意识，系统配置，审计，测试，安全开发等方方面面都是围绕着如何保护预设目标展开。该标准也是适用与对于希望将整体环境安全水平提高的企业，只是在实际建设过程当中需要企业预设期望保护的对象，并参照PCI DSS的要求进行安全建设。值得一提的是PCI DSS在其第11.2条要求当中提及了企业需要定期的执行内部和外部的安全扫描以评估企业当前存在的安全漏洞评估识别所面临的安全风险，由此可见安全扫描在IT安全建设领域是最基本的安全工作，也是被广为推荐的工作。

与其他 IT 领域的建设一样，信息安全建设是一个长期的工作， 它随着信息安全的不断发展，随着信息安全热点的不断更替变化需要企业自身作出及时的进行调整。对于企业来说把握信息安全动态最有效的方式是参考业界的标准或者最佳实践，因为这样可以节省大部分企业在研究信息安全领域发展的人力与物力的投入。对于与支付或者电子商务相关的企业可以参考或者关注 PCI DSS；对于软件开发类相关的公司可以参考 FIPS 140-2（关注在密码算法和密码模块评估和测试的标准），以及 Open Web Application Security Project 简称 OWASP 所开发和维护关注在 WEB 应用程序安全设计、编码与测试相关的标准。

随着网络信息化的发展，信息安全问题已经成为人们，不仅是信息安全领域的专家所关注的热点。面对来自网络的各种威胁，相应解决问题的方法、工具和手段也随着人们的重视而增强。网络中没有绝对的安全，但是我们可以做到最大限度的避免网络中出现的问题和安全隐患，外部安全扫描就是其中一种最优其有效的解决企业对外提供服务的基础设施所面临安全风险的方法。atsec 提供的外部安全扫描服务，能够全面的识别可能会遭受自外部的攻击的脆弱性以及自身开发的程序所存在的安全问题，所有已经核实或者潜在的脆弱性将会在报告当中进行全面的展现，并且我们为每一个脆弱性都提供详细的解决方案。在 IT 安全领域建设多年的实践过程当中，atsec 一直关注信息安全的动态，针对防范外部攻击、骇客入侵等活动，我们沉淀了丰富的应对解决方案，我们期望能够将沉淀的内容及经验为更多企业的信息安全建设做出贡献。

相关资料分享

atsec 外部安全扫描协议：[http://www.atsec-information-security.cn/downloads/rfi/Commission_Contract_for_External_Security_Scan.doc]

atsec 外部安全扫描执行摘要样例：[http://www.atsec-information-security.cn/downloads/presentations/atsec 外部安全扫描执行摘要样例.pdf]

atsec外部安全扫描技术报告样例：[http://www.atsec-information-security.cn/downloads/presentations/atsec外部安全扫描技术报告样例.pdf]

相关 atsec 信息链接

atsec_weibo：[http://weibo.com/atsecchina]

atsec_blog：[http://blog.sina.com.cn/u/2415017805]

艾特赛克（北京）信息技术有限公司
北京市海淀区上地七街1号
2号楼119室 100085
电话：+86 10 84834011
传真：+86 10 82890017
Email：info_cn@atsec.com