PCI DSS 成功指南

PCI DSS 成功指南

目前主要的信用卡公司已经进行了委托，所有的会员、商家和服务提供商存储、处理以及传输持卡人数据都必须遵守支付卡行业（Payment Card Industry，PCI）的“十二诫律”——12 条最佳做法组成的指南。另外，到 2007 年 9 月 30 日，所有的二级企业——每年处理 15 万 Visa 或者 MasterCard 交易的商家或者每年交易量超过一百万的商家——必须遵守这些标准。不幸的是，由于资金数量、时间和精力的要求，遵守 PCI DSS 的难度非常高。本指南将介绍难度较大的 PCI DSS 的要求，并提供一些帮助企业遵守 PCI DSS 规定的技巧。

PCI 最难五条规则

PCI DSS 的所有要求的说明都相当明确，不像萨班斯法案（SOX）的规定。SOX 没有提供如何保护信息资产的任何详细指导，而且可以由企业和法规审计单位自由做出不同的解释。然而，企业仍然觉得遵守 PCI DSS 很难

- PCI 最难五条规则指导

PCI DSS 规则详解

尽管 PCI DSS 非常全面，这些要求中还是有写可能出错的地方；任何一条不能满足都表示企业不能遵守法规。另外，即使 PCI DSS 提供了详细的要求，它还是会被不同类型的企业以不同的方式解读。本部分将介绍不易遵守的 PCI DSS 要求，分析为什么有的企业中会产生问题，并讨论解决这些困难可以采取的措施。

- PCI DSS 成功策略：第三条规则
- PCI DSS 成功策略：第十一条规则
- PCI DSS 成功策略：第八条规则

- PCI DSS 成功策略：第十条规则
- PCI DSS 成功策略：第一条规则

PCI DSS 成功策略之总结

PCI 的设计是为了从开始接收到生命周期的终结保护信用卡数据。这道门槛对于互联网业务的工具来说很高，这些公司都非常依赖信用卡来处理产品和服务的销售。只要一次安全泄漏就会造成业务底线以及声誉的重大伤害，而这种伤害可能是永久性的。理解“十二戒律”中的那些是最困难的可以帮助企业避免在错误的思想或技术的实施上浪费时间、资金和精力。

- PCI DSS 成功策略之总结：降低风险的挑战

PCI 最难五条规则指导

大家都知道，目前主要的信用卡公司已经进行了委托，所有的会员、商家和服务提供商存储、处理以及传输持卡人数据都必须遵守支付卡行业（Payment Card Industry，PCI）的“十二诫律”——12 条最佳做法组成的指南——或者可能的风险处罚，甚至是信用卡权限的终止。另外，到 2007 年 9 月 30 日，所有的二级企业——每年处理 15 万 Visa 或者 MasterCard 交易的商家或者每年交易量超过一百万的商家——必须遵守这些标准。不幸的是，由于资金数量、时间和精力的要求，遵守 PCI DSS 的难度非常高。

这一系列指南将介绍难度较大的 PCI DSS 的要求，并提供一些帮助企业遵守 PCI DSS 规定的技巧。

PCI DSS：企业的难点在哪里？

PCI DSS 的所有要求的说明都好像相当明确，不像萨班斯法案（SOX）的规定。SOX 没有提供如何保护信息资产的任何详细指导，而且可以由企业和法规审计单位自由做出不同的解释。然而，企业仍然觉得遵守 PCI DSS 很难。在由 VeriSign Inc.进行的一项调查中，研究人员发现企业很可能不能遵守 PCI 要求第三条。评估不成功的企业中有 79%不能满足保护存储数据的要求。

第三条：保护存储数据	79%
第十一条：定期测试安全系统和程序	74%
第八条：向每个访问电脑的人分配单一 ID	71%
第十条：跟踪/监控网络资源和持卡人数据	71%
第一条：安装并维护防火墙配置，保护数据	66%

为什么这些地方出现问题？

尽管 PCI DSS 非常全面，这些要求中有 12 个可能出错的地方；任何一条不能满足都表示企业不能遵守法规。另外，即使 PCI DSS 提供了详细的要求，它还是会被不同类型的企业以不同的方式解读。我们将介绍上面提到的不易遵守的 PCI DSS 要求，分析为什么有的企业中会产生问题，并讨论解决这些困难可以采取的措施。

（作者：Craig Norris 译者：Tina Guo 来源：TechTarget 中国）

PCI DSS 成功策略：第三条规则

PCI DSS 第三条规则是保护存储数据。

从商家接收到用户的信用卡信息的那一刻起，所有的信用卡数据都必须加密。在 2007 年 3 月的 Visa 会议上进行的 National Federation of Independent Business/Visa 调查中，有些小业主说他们相信他们在保护客户数据方面作的很好，尽管相反的事件经常发生。在保护了客户数据的回答这种，超过 25%的人把用户数据记录在不安全的文件中，36%的被调查者在他们的商店中接收信用卡数据。

这条要求的最大问题之一是商家必须准确地知道信用卡数据是从哪里开始流出的、在网络的哪些部分移动和停留的以及在网络上时的状态。这就是识别并检查所有的桌上电脑、笔记本电脑、服务器和处理持卡人所有信息的数据这么重要的原因。这包括所有的包含了信用可数据的数据库文件和/或 SQL 表格，而没有提到创建或者访问信用卡数据的所有应用系统。不管接触信用卡信息的是哪种系统，都必须要加密。

如何满足 PCI 第三条规则

正如上面所提到的，首先要确认所有接触持卡人数据的系统，因为这些系统会包含在最终的 PCI DSS 审计或者法规确认的范围内。了解持卡人的区分以及他们如何使用防火墙和网络过滤控制也非常重要。这样的安排可能确定相邻的系统是否也在 PCI DSS 法规确认的范围中。你可能会对保留用户数据的系统总数感到吃惊，这些系统包括数据资料库、开发服务器、中间件和备份系统，这个数据非常庞大。

下一步，对经过企业的信用卡数据流进行存档，并确认业务功能。市场部，例如，可能需要用户数据，但是和信用卡信息不相关。从起点处跟踪数据——甚至是从客户或者第三方——到数据被处理的位置或者到离开企业网络的位置。还要确认所有和企业架构和应

用相连的电脑和网络。这包括业务单位、厂商、合作伙伴和远程员工系统的网络连接。所有流动的信用卡数据都应该使用 SSH、VPN 或者 SSL/TLS 等方法进行加密。

如果你对 IT 部分准确分辨敏感数据的能力不太信任，还有一些很好的数据丢失防护工具可以提供帮助。这些工具可以筛选通过企业的数据，并准确地报告哪些系统接收了这些数据、数据在系统的什么位置以及谁访问了数据。一旦了解了这些，就需要检查企业的访问控制，执行“必须了解”的策略。另外，还要看一下是可能确认那些系统存储了敏感数据，是否可能把这个数量降到最低。

（作者：Craig Norris　译者：Tina Guo　来源：TechTarget 中国）

PCI DSS 成功策略：第十一条规则

PCI DSS 第十一条规则：定期测试安全系统和程序。

很多企业很少或者没有对管理他们的网络和面向互联网的 Web 网站应用的安全控件进行定期测试。没有定期运行内部和外部网络扫描来确认漏洞在后门向黑客和恶意代码开放大门的时候就会付出很大的代价。企业可能会在某些时间受到保护，但是新的漏洞每天都会出现，这也是为什么网络应该不断地打补丁并加固。根据美国国土安全（Homeland Security）的 国家网络安全部门（National Cyber Security Division）提供的国家漏洞数据库（National Vulnerability Database）资料，互联网上每天平均会出现 19 个漏洞。

需要定期测试系统和程序的一个很好的例子是 TJX Companies Inc 的数据安全泄漏事件。TJX 泄露事件最终归结于不安全的无线网络。根据华尔街日报的报道，调查人员认为黑客可以使用笔记本电脑和压缩天线（telescope-shaped antenna）绕过老旧的安全技术并渗透到 WLAN 网络。这家拥有 174 亿资产的零售商的无线网络的安全措施甚至低于很多家庭网络用户。在 18 个月中，TJX 都不知道它已经受到攻击了，这种攻击可以允许恶意黑客下载至少 4570 万的信用卡和借记卡号码。

如何满足 PCI 第十一条规则

当提到扫描信息系统的漏洞的时候，确定要使用可以发现有线和无线网络上设备漏洞的工具和技术。和无线协议、弱加密方法和员工安全意识却犯相关的安全风险的数量很大。破解方法已经变得非常先进了，使用网络上的免费开源工具就可以进行。

对没有使用最新安全更新的系统地成功攻击的数量一直很大。除了系统补丁程序，对网络和应用安全威胁最大的保护是坚持使用可以观察网络上所有应用和设备、确认漏洞并提供修复信息的漏洞扫描器。但是，扫面企业网络的漏洞还不能表现所有问题，只能发现

已经遇到的问题或者至少发现。扫描，虽然很有希望，但是可能没有必要提供真实的类似攻击的渗透测试项目所提供的功能。

为了了解它是否准备好了，（PCI DSS 要求并）命令企业必须每年执行信息系统的渗透测试，测量系统可承受工具的程度。这种类型的测试实际利用漏洞，更好的量化某种特殊发现的真实风险。根据零售数据安全 2005 基准研究（The Retail Data Security 2005 Benchmark Study）的报告，只有 51%的零售商执行了网络渗透测试。令人吃惊的是，调查回应者的 14%的指出他们遭受过客户数据安全泄漏。漏洞扫描可以查看已知的漏洞，但是没有解决成功入侵的因素。测试应该包括深度调查，可以显示对企业资产的真实威胁。

此外，当提到测试程序的时候，所有可能影响到进入和流出过滤规则的变化都应该在对防火墙、路由器、VPN 和 WLAN 设备进行调试前，通过正式的测试程序。这些变化因为恰当的原因都应该被认真检查，而且应该管理新发现的安全风险。信息系统环境应该总是变化以帮业务达到目标；因此，所有的变化都必须不断地检查并存档。

（作者：Craig Norris　译者：Tina Guo　来源：TechTarget 中国）

PCI DSS 成功策略：第八条规则

PCI DSS 第八条规则：为访问计算机的每个用户指定独立 ID

对 PCI 法规比较关注的一点是对谁做了什么，以及时间的可追溯性和说明。企业认识到用于满足这条规则的主要技术是用户名和密码管理，而且这些技术的使用也不是很困难。为了满足规则，合并可以自动完成任务的工具，或者分派技术员工来解决问题。大型网络中存在很多进入点的各种环境，包括防火墙和 VPN 访问。如果没有合适的架构，这些不同的选择使跟踪用户帐户的信息系统上的行为变得很困难。这些相同的企业可能不能监控所有变化的鱼面密码策略。

如何满足 PCI 第八条规则

企业必须有能力识别、记录所有用户并管理对包含信用卡信息的信息系统和应用的访问。企业必须为访问计算机的每个人创建独立 ID。公司还必须拥有（全体员工签署的）书面政策，指出所有的 ID 和信任状（credential）都只能被指定的人员使用。企业需要有能力核实谁想要访问资产。他们还必须控制哪些员工有权限察看、修正，并且这些行为是居于企业任务的。

管理方面要确保老化的密码上执行的策略。例如，如果公司策略说明所有的密码都必须每 45 天更改一次，他们必须有能力证明密码确实更改了。另外，企业还应该能够证明他们想新雇用的员工提供密码的程序是可以重复的，还应该可以在员工不再为企业工作的时候移除密码。

PCI DSS 还要求使用双因素认证来识别需要访问资源的远程用户，不管他们是员工、管理员还是第三方。虽然帐户名和密码是最简单最经济得网络登录认证方法，但是企业现在开始认识到这种方法的缺点。密码可以通过使用字典攻击被猜测或者破解，或者用户也会被欺骗向其他人透漏他们的密码。阻止社会工程攻击并减少和密码相关风险的方法之一

是采用双因素认证。如果用户需要输入密码并提供附加信息，例如智能卡或者令牌上的 PIN，那么黑客就不能只使用密码进入网络了。双因素认证可以通过合并用户所知道的（例如，密码）、用户所拥有的（ATM 卡）或者用户的身份（指纹）来建立。

最后，至关重要的是企业使用企业范围内的认证构架，而这个构架可以对用户安全连接到网络地方式进行控制。这个构架可以构建，也可以购买。它不应该只能被用于认证访问资源的用户，而且应该可以根据业务的要求帮助限制对资源的访问。这样的做法要求开发一套可以重复的程序，还有保护用户身份和数据的技术和策略。把用户限制在“需要知道”的基础上可以帮助降低风险。

（作者：Craig Norris　译者：Tina Guo　来源：TechTarget 中国）

PCI DSS 成功策略：第十条规则

PCI DSS 第八条规则：跟踪并监控对网络资源和持卡人数据的访问。

很多企业都有独立的网络，而且必须手动跟踪每个系统日志文件，才能遵守 PCI DSS 的规则。过滤个别的系统日志还不是很耗费时间的过程，但是这也在 IT 中主要的耗费精力的任务，特别是当需要判定攻击起因的时候。企业必须跟踪并监控对网络资源和持卡人数据的访问，包括实时、每天的活跃活动。除了管理这些日志，大部分的企业并没有良好的策略可以解决各种信息被记录的问题，而企业也没有办法延续日志数据的完整性。当提到访问信用卡数据的时候，企业不应该只是拥有查帐所引（audit trail），还应该向绝对需要了解的人提供敏感数据。

如何满足 PCI 第十条规则

虽然分析日志和事件数据在 PCI DSS 中有详细说明，但是企业监控这些事件也是很好的做法。在普通的信息系统环境中，事件数据是分散的，数量巨大，需要大量时间来解释。大部分的操作系统，默认都有分析事件的工具，但是他们只提供基本的功能，因此，当特定的严重事件被记录时，例如对持卡人信息的非授权访问，没有办法警告 IT 人员。这些工具所提供的事件浏览和过滤功能在很大程度上都是受限制的。

但是，有很多很好的软件或者硬件的安全信息管理（security information management，SIM）可以提供全面的日志管理。SIM 工具可以集中处理事件，使事件数据的聚合和收集自动化，发布警告并提供相当详细的报告功能。当聚合事件的时候，SIM 不仅可以帮助正常网络活动基线的创建，还可以提供内置的规则，可以进行分类以及最后的警告和程序的触发。很多安全信息管理产品还提供默认规则设置，根据 PCI 的要求对事件进行分类。

（作者：Craig Norris　译者：Tina Guo　来源：TechTarget 中国）

PCI DSS 成功策略：第一条规则

PCI DSS 第一条规则：安装并维护防火墙配置，保护信用卡持卡人数据。

安全专家第一眼看到这条规则，简单在网络边界上安装防火墙，然后认为就万事大吉了。不完全是。很多人都没有认识到 PCI DSS 第一条要求指明了企业不仅需要过滤进出流量规则的正确配置和存档的正在运行的防火墙，而且还要使用受信区域（例如 DMZ）以及使用在无线网络和持卡人数据环境至记那安装的边界防火墙。在 PCI DSS 的第一条规则的细节中只有很少的部分可以忽略。

如何满足 PCI 第一条规则

企业需要彻底地检查控制进出网络的流量的防火墙规则和策略。很多防火墙在初始的网络安装后，在很长的时间内就再也没有碰过了。因为业务应用需要和客户要求总是在变化，很多规则都要调整以适应附加端口和服务的启动，允许受信任和不受信任网段之间的开放通讯。

这些设备上的所有变化都必须经过同意，正确的存档并不断地检查，确保他们都经过了加固并且只允许安全信息在网段之间流通。这种保护得存档配置标准和证明网络做法正确的特定存档都是强制性的。

最后不要忘了配置必须提供资产存储、传输或持卡人数据处理的安全，而这些包括来自无线和移动设备的信息的恰当网络分段。

（作者：Craig Norris 译者：Tina Guo 来源：TechTarget 中国）

PCI DSS 成功策略之总结：降低风险的挑战

PCI 的设计是为了从开始接收到生命周期的终结保护信用卡数据。这道门槛对于互联网业务的工具来说很高，这些公司都非常依赖信用卡来处理产品和服务的销售。只要一次安全泄漏就会造成业务底线以及声誉的重大伤害，而这种伤害可能是永久性的。

理解“十二戒律”中的那些是最困难的可以帮助企业避免在错误的思想或技术的实施上浪费时间、资金和精力。

另外，了解 PCI 不是和企业的员工数量以及年收入相关的也很重要，这样企业就必须不能只把规则当作清单，而是作为开发风险管理程序的行为指南。执行有力的安全策略、采用日志和漏洞管理技术、恰当地构建网段并通过使用防火墙保护边界在帮助企业遵守 PCI 法规方面起到很大的作用。。

（作者：Craig Norris　译者：Tina Guo　来源：TechTarget 中国）