atsec NEWS
the information security provider
09/2011

2011 年度 atsec 信息安全培训活动回顾

培训是一种有组织的标准、知识、信息等传递和分享行为，atsec 作为专业的信息安全服务机构，积累了丰富的信息安全实践经验，通过公开或定制化的培训课程有效的对各个行业的安全、技术专员进行信息安全相关知识以及相关标准的解读，为信息安全业界尽可能的提供信息分享和贡献。

2011 年 1 月 14 日，atsec 在中国信息安全认证中心举办年度信息安全培训活动，本次培训的重点专注在 FIPS 140 和支付卡行业数据安全标准 PCI 以及相关技术领域的最佳实践。本次培训特别针对 PCI DSS 最新版本标准 v2.0 和原有版本的比对进行了详细的分析和实施分析，得到了产业内的高度关注。

2011 年 7 月 13 日至 7 月 15 日，atsec 在北京成功举办为期三天的专注在通用评估准则（” Common Criteria”）的培训，吸引了中国业界专家、认证和测评机构，知名厂商的共同参与。

2011 年 8 月 11 日和 12 日，atsec 在上海举办围绕 PCI DSS 展开的培训课程，重点专注在 PCI 合规建设的案例分析和 atsec 风险评估知识分享。

此外，atsec 全球范围的培训工作也如火如荼的展开，特别在通用评估准则（CC：Common Criteria）和 FIPS 140 领域，在美国和欧洲召开了多次研讨会。atsec 无疑是此领域产业的领导者。

atsec 作为全球化发展公司，为客户提供广泛的信息安全服务，吸取国外领先的技术和先进的思想帮助中国客户和合作伙伴了解国际的信息安全动态，为学员们带来最新、最快、最正确的标准解析和案例分析。

atsec 每年进行不定期的培训，根据客户不同的需求定制不同的课程。多年来，atsec 本着贡献、开放的态度，与我们的客户及合作伙伴共同推动和发展国内信息安全事业。将诸多的信息安全技术知识和经验与业界同仁分享。培训的课程大多以书面知识讲解、互动交流以及实际操作等多种形式展开。培训的内容主要依据信息安全标准 PCI DSS、FIPS 140、Common Criteria、渗透测试、风险评估、NASPO 等国际、国内标准和法律法规展开。atsec 的信息安全培训吸引了诸多业界同仁的关注和参与，包括来自安全厂商、银行、支付卡产业的服务提供商、支付应用系统开发商、大型商户，以及测评机构等企业的技术骨干。

每次培训后 atsec 都会进行内部的总结和交流，根据学员们反馈的不同需求和意见，对培训的内容、方式、语言等进行优化和改进。atsec 希望每一次的培训活动都能为产业内的同仁们构建一个良好的交流平台，让每一位学员在这个平台上分享技术、交流心得！

atsec 计划将在 2011 年年末开展以“渗透测试”为主题的培训活动，敬请关注。

更多培训信息请点击浏览：http://www.atsec-information-security.cn/cn/trainings.html

如何高效地执行信息安全风险评估

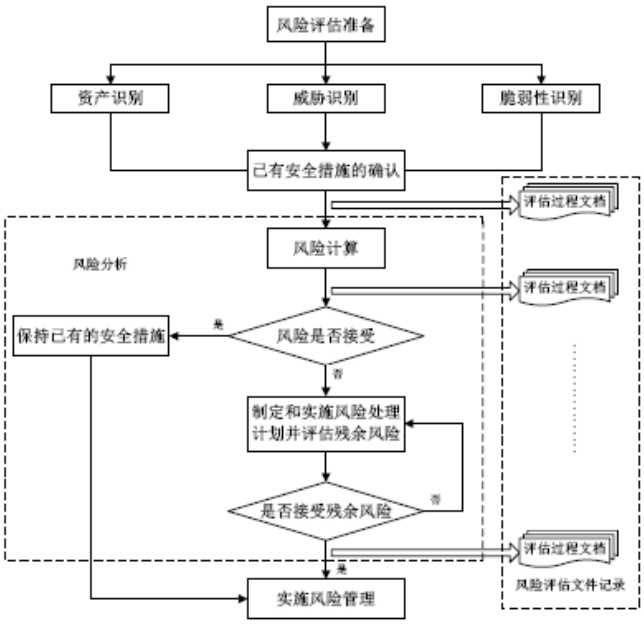
atsec 高级咨询顾问 高向东

信息安全风险评估工作对于组织进行信息安全风险的有效管理、识别并修复安全风险点具有非常重要的意义，同时也是组织为满足安全合规管理的要求之一，如当前主流的信息安全管理体系 ISO/IEC 27001、PCI-DSS 数据安全标准等均有明确的风险评估要求。而在实际风险评估工作的执行过程中，组织难免会走入一个极端：会因为合规或监管的要求而在极短时间内执行完成，因时间和人力等方面的分配，往往难以有效地发现和准确评价各种威胁的影响，使得风险评估流于形式。

在执行信息安全风险评估的过程中，有些组织会将风险评估工作委托给专业的安全风险评估机构来执行。诚然专业评估机构具有很强的方法论和知识积累，然而如果对每一个客户都用完全相同的方法和知识库，难免会出现对某些风险评价的偏差甚至缺失。

笔者认为，信息安全风险评估是一个专业性很强的工作，组织除了依赖于专业评估机构的能力以外，组织本身仍然需要明智地进行管理和影响，使得组织通过该过程可以真正有效地管理所面临的风险。

在风险评估的执行过程大体可以分为三个阶段，评估准备与识别、风险的评估与计算以及风险结果处置。准备与识别阶段主要进行资产梳理、威胁识别以及脆弱性识别等工作；评估与计算阶段主要基于识别到的风险要素和措施，进行风险的评价和计算；而处置阶段刚基于评估结果进行有效的风险处理，所采取的方法通常包括接受风险、降低风险或转移风险等。为便于理解，下图是 GB/T 20984-2007 标准中对风险评估过程，从整体上对风险评估工作所涉及的工作要素进行了说明。



一、组织所面临风险的定制化

在风险评估的准备阶段， 需要针对组织当前的情况进行大量的信息收集，再加上对信息的分析与整理，这将占用大量的时间资源。而如果不进行梳理，则无法达到风险评估的预期效果。而制定适合组织当前状况的评估项，相关的实践经验如下：

1、扩展安全威胁信息库以覆盖组织面临的主要风险

如基于常见的信息安全风险来开展，难免存在对于威胁的忽略和偏差。组织可以从以下角度来考虑威胁数据库的构建：

- 威胁的种类

比如可以从对组织产生影响的角度，扩展组织所适用的威胁库分类。笔者认为威胁库的积累对于风险评估最终的效果将有直接的影响，建议组织在信息安全风险评估机构的选择过程中充分考虑评估机构对于信息安全知识，尤其是威胁知识库的积累。

借助于遍布全球的知识资源，atsec 所采用的知识库体系可覆盖到信息安全风险的方方面面，如合规风险、物理安全、人员安全、安全管理、技术架构、介质管理、权限管理、密码管理、安全意识等多个领域。通过全面的安全风险分析，使得组织可以非常有针对性地制定当前以及未来的信息安全建设规划。

- 威胁的来源

组织在确定威胁的过程中，除了考虑自身面临的风险外，推荐从风险合规的角度来扩展威胁的信息来源。atsec 可以在风险评估过程中帮助组织梳理并明确组织所处行业的监管要求，指导组织建立或完善统一整合的管理体系，并有效地吸收和融合 PCI、ISO/IEC 27001、ISO 9001、ITIL、SAS70 等标准，形成全面且有针对性的威胁信息库，使评估结果达到事半功倍的效果。

2、高效地进行资产的识别与评价

对于组织的信息资产，尤其是数据资产，难以进行有效地衡量和梳理。然而，风险评估过程中则需要对所影响的信息资产的价值纳入到评价体系。由此看来如何明智地组织资产的评价体系，并对资产进行合理评价是一个具有挑战性的工作。在该过程中，atsec 的执行经验如下：

- 建立有效的资产层次

通常的资产层次可以从物理位置（如 XX 组织的生产机

房），到物理概念上的资产（如 XX 机房的 XX 服务器），再到操作系统，进而到应用软件，最终到其中的数据。经过多层次的资产划分后，其好处是使得威胁与资产具有了明确的关联关系，便于后续的风险评价。

- 有效地使用“资产组”的概念

在建立资产层次后，也会带来资产类别和梳理过程的工作量的成倍增加。在 atsec 执行风险评估的过程中，会充分考虑低层级资产的梳理难度，更多地从业务流程划分的角度进行归类，在最大程度上使用“资产组”的概念，尽最大可能使用组合的方法降低难度。

3、快速收集与评价组织的管理体系

风险评估的执行更多地侧重于发现安全管理过程中的差距，管理体系梳理与具体评价应更多地由内部或外部审计来完成。然而，在此过程中也需要有一定的介入并给出初步评价，以便于安全流程等方面的实际评估。

二、科学地提升执行效率和准确性

在风险的评估与评价阶段，项目团队的成员应把绝大部分精力投入到风险项的识别和级别定义，除了依赖于执行者的信息安全评估的经验外，使用有效的方法论和工具方法对于提升执行效率和准确性也具有非常重要的意义。

1、建立有效的风险分析模型

在风险评估过程中，atsec 所使用的风险分析模型会包括多个层面，以更有效地进行风险评价。模型方法如下：

- 风险发生的可能性
- 初步的控制措施
- 风险发生对客户业务的影响
- 风险发生对客户品牌的影响
- 风险发生对客户收益的影响

对于具体的分析过程，由评估人员基于访谈情况、渗透情况以及相关的信息输入，从品牌、收益和客户三方面的影响进行展开。每一选项的赋值基于方法论中的准则进行确定，下图为整个风险评估过程中，对数据库和应用系统存在威胁的评定示例：

Scenario Index	Scenario	Description	Threat	Vulnerability	Existing count	Things to remember for "Measures"	Incident likelihood (EW)	Main Asset	Brand impact (BI)	Financial impact (FI)	Customer impact (CI)	Potential damage (SA) = (BI + FI + CI)/3	Risk (EW * SA)
数据库													
DB	数据库安全	数据安全											
DB_r1	DB2数据库存在安全漏洞		数据库遭到攻击	机密信息泄	无	安装缺失的数据库补丁	B - low	DB2	4 - large damage	5 - very large damage	2 - small	4 - large damage	medium
DB_r2	MSSQL数据库存在安全漏		数据库遭到攻击	机密信息泄	无	安装缺失的数据库补丁	B - low	MSSQL	4 - large damage	5 - very large damage	2 - small	4 - large damage	medium
DB_r3	相同的密码应用在不同		数据库遭到攻击	相同密码的系	无	引入集中管理的认证机制	C - medium	数据库系统	1 - very small damage	3 - medium damage	1 - very small	2 - small damage	medium
DB_r4	没有密码或则或者弱的		数据库密码猜测	数据库账户密	无	引入密码策略	C - medium	数据库系统	1 - very small damage	1 - very small damage	1 - very small	1 - very small damage	small
应用													
App_vul	应用系统安	应用系统层											
App_vul_r1	跨站(XSS)安全漏洞		互联网攻击	威胁客户的安全，业	无	研发人员对应用程序进行修改并定期对应用程序进行安全检测	D - high	业务系统	5 - very large damage	1 - very small damage	5 - very large	5 - very large damage	very large
App_vul_r2	CGI通用的Cookie注入漏洞	CGI Generic Cookie	互联网攻击	威胁客户的安全，业	无	研发人员对应用程序进行修改并定期对应用程序进行安全检测	B - low	业务系统	1 - very small damage	2 - small damage	3 - medium	3 - medium damage	medium
App_vul_r3	服务端远程执行	CGI Generic SSI	互联网攻击	业务系统被注入恶意	无	研发人员对应用程序进行修改并定期对应用程序进行安全检测	C - medium	业务系统	3 - medium damage	3 - medium damage	2 - small	3 - medium damage	medium

2、使用半定量化的风险计算方法

因威胁本身具有不断变化和难以测量的性质，推荐明智地使用半定量化的测试方法。在具体的执行过程中，atsec 的做法是通过对每个威胁的评估结果给出半定量的评级，并进一步通过风险计算方法使最终的评估结果更精确。

3、使用自动化的风险计算工具

基于风险评估在执行过程中，atsec 使用自有开发的计算工具，以最大程度上节省风险计算所占用的工作量。

4、最大限度地使用辅助工具

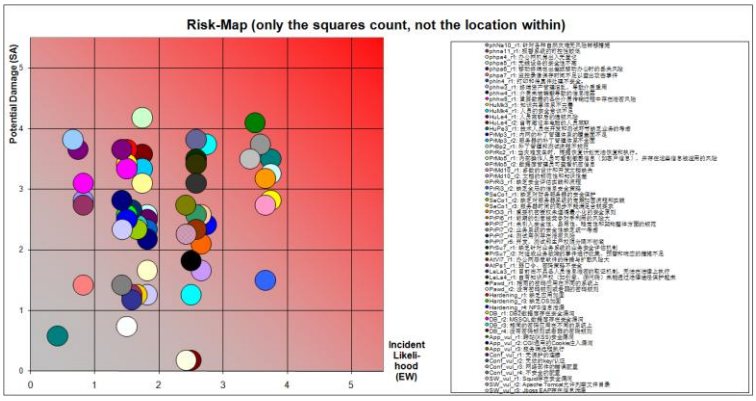
在对技术类威胁的评估过程中，如关键帐号和口令安全性，通过管理访谈方法通常难以做出准确的判断。atsec 则会在类似的过程中尽最大限度地使用各种辅助工具和手段，比如密码安全性验证、服务器的技术漏洞等。

三、评估结果的高效使用

在对所有的威胁完成风险评估后，如何有效地将风险结果转化为组织进行高效改进的发动机呢？

1、自动、清晰地呈现风险发现与结果

在发现并对信息安全风险进行评价后，自动地呈现风险结果与发现不仅可以极大地节省风险评估过程中的资源，也将使得管理层清晰地知晓关键的信息安全风险。这对于信息安全风险评估项目的收益具有非常重要的意义。在风险评估过程中，atsec 会通过自动化工具全面展现风险评估的发现与结果，如下图所示：



2、全生命周期的风险管理

一旦一个风险被识别出来之后，将对其整个过程进行管理和控制。通常的处理方法包括：风险降低（如通过技术手段降低其影响或可能性）、风险转移（如购买保险或通过第三方合同转移）和风险接受（管理层正式接受风险及其影响）等。建议组织在执行过程中使用自动化的工具跟踪每一个风险的最终处理方法，以避免风险项被忽略和措施不到位的情况。

3、自上而下的管理决策

对于识别到的风险，需要管理层投入资源进行处理，在此看来自上而下的管理决策非常重要。atsec 在风险评估管理过程中，会通过自动化的工具列举出来，然后需要组织的管理层首先进行低级别风险的接受，最后将工作着眼于中、高级别风险整改措施的确定。

4、通过投入产出比指导安全措施的制定

在排除可接受的风险后，所残余风险项的管理也是风险评估后期的难点之一。在此过程中，atsec 推荐从投入产出比的角度考虑措施的制定。笔者认为，在整个信息安全风险评估过程中所做出的努力不仅仅是一项时间、金钱和人员的投入，而是一项为组织避免由安全风险带来更大安全损失的核心。能做到这个的关键一点是在风险整改措施的投入方面，应至少要小于所避免的安全损失，这就要求借助于半定量化的指标来指导安全措施的选择，以达到最大的投入产出比。

在整个风险评估过程中，atsec 采用的半定量化的方法和结果仍然可用于达到此目的。举例来看，对于识别出的“应用层 XXX 漏洞”的整改措施，则可以基于应用的价值以及该漏洞的风险值确定该风险的损失值，而安装 WAF 设备、使用商业应用层漏洞扫描工具、使用开源工具进行应用扫描、由开发人员进行安全代码检查等措施每个的投入也可以从工作量和确认，这将使得最终的措施或措施组合为组织产生更大价值。

总结：

对于风险评估这样专业性很强的工作，建议组织从信息安全经验和积累的角度出发，选择、借鉴并融合业界优秀风险评估机构的经验和实践，以最大化风险评估的收益。对于执行策略，应充分融合内、外部资源，明智全面地覆盖所有威胁，并通过执行过程的自动化和投入产出比的优化，使风险评估工作真正地成为应对各类风险以及风险合规的利剑。

atsec 是一家独立且基于标准的 IT（信息技术）信息安全咨询和评估服务公司，它充分结合了丰富的技术知识和国际经验，可以为组织提供具有商业导向的信息安全服务。atsec 利用其对安全保障、应用和标准方面的丰富专业知识，将协助组织建立完整的安全管理流程，进而有效地管理安全风险，改善数据和产品，以确保业务流程的可靠性。

PCI DSS 合规建设 ASV 扫描介绍

atsec 高级咨询顾问 陈谨运

PCI DSS 介绍

PCI（Payment Card Industry）中文全称为：支付卡产业。在这个产业里存在一个标准组织，称为：支付卡行业安全标准委员会，英文简写为 PCI SSC（Payment Card Industry Security Standards Council）。PCI 安全标准委员会是由国际知名的五家支付品牌共同建立而成，他们是美国运通（American Express）、美国发现金融服务公司（Discover Financial Services）、JCB、全球万事达卡组织（MasterCard）及 Visa 国际组织。PCI SSC 一共维护了三个安全标准：PCI DSS（Payment Card Industry Data Security Standard 支付卡行业数据安全标准）、PCI PA-DSS（Payment Card Industry Payments Application Data Security Standard 支付卡行业支付应用数据安全标准）以及 PTS（PIN Transaction Security PIN 传输安全标准）。从下图可以很清楚的反应这三个标准之间的关系。

无论是 PTS 还是 PCI PA DSS，其最根本的目的是为了使最终的客户能够满足 PCI DSS 的要求。（关于 PTS 和 PA DSS 更多的介绍可参见 PCI 官方网站 www.pcisecuritystandards.org 和 atsec 官方网站 www.atsec-information-security.cn）。

在PCI DSS第11.2.2中有这样的要求“Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).”其转译中文意思是：每季度由PCI SSC认可的授权扫描服务商(Approved Scanning Vendor) --- ASV执行外部的脆弱性扫描。

什么是ASVs

授权扫描服务商是经过 PCI SSC 认可的，为商户和服务提供商的对外提供服务的互联网环境执行脆弱性扫描的组织，它的目的是为了验证商户和服务提供商遵守一定的 PCI DSS 要求（PCI DSS 11.2 要求）。

PCI DSS 对于 ASVs 的要求

对于ASVs而言，PCI SSC维护了一套认证的流程，详细的认证流程可参见PCI SSC的指引文件。根据要求ASVs每年都需要进行资质的重新认证，认证的结果可以从PCI官方网站上查询到，详细地址参见：

https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

对于ASVs的认证，PCI SSC除了对公司的资质要求以外，扫描工具也需要经过 PCI SSC 的认可。除此以外执行 ASV 扫描的人员则需要通过 PCI SSC 的 ASV 在线考试。

ASV 扫描的流程

根据PCI SSC的规定，所有ASV的执行过程和流程都应该要满足“asv_program_guide_v1.0”的要求。该指导文件描述了ASV扫描流程中的不同角色，扫描范围的确定，脆弱性分类，扫描报告内容描述，误报处理，报告的交付和完整性保护，质量保证等内容。

ASV 范围的确定

在执行 ASV 扫描之前，执行扫描的人员需要与客户一起去确定 ASV 扫描的范围。通常客户需要提供其对外提供服务的所有 IP 地址列表，网络拓扑图以及相关的资料以便扫描人员能够根据 PCI DSS 要求判断哪些系统组件应该要在扫描的范围之内。按照 PCI DSS 标准的要求：所有对外提供服务的涉及持卡人信息传输，处理或者存储的系统组件都需要每季度执行 ASV 扫描。这里的系统组件包括但不限于服务器，网络设备，安全设备。

在初步确定 ASV 扫描范围之后，扫描人员需要使用 ASV 扫描工具的“探测”功能去探测目标系统以及与其相关联系统组件的状态。在这个环节当中，ASV 扫描工具会自动化的去识别与预设目标相关联的系统组件的活动状态，所以“探测”扫描发现的 IP 地址数量通常会比预设目标的 IP 数量会更多。这时候扫描人员就需要根据发现的结果与客户进行讨论以最终确认 ASV 的扫描范围。

如何判断是否通过 ASV 的扫描

对于ASV扫描的结果，很多客户都会关心什么样的条件能够通过ASV扫描，是否有统一的标准？

根据PCI SSC“asv_program_guide_v1.0”的描述，所有包含高危严重级别的脆弱性和任何违反PCI DSS的功能或配置的脆弱性都将不能通过ASV的扫描。

以下是CVSS评分和NVD严重级别与ASV扫描结果的对应关系：除了少数特定情况，任何CVSS分值大于或者等于4.0的脆弱性都不能够通过ASV扫描。

CVSS 分值	严重级别	ASV 扫描结果	指导
7.0 -- 10.0	高危	失败	为能够通过 ASV 扫描，这些脆弱性被修复并且在脆弱性修复之后需要再次执行扫描。组织应采取以风险级别为基础的方法来纠正这些漏洞，按照风险的危害程度最关键的（CVSS 分值为 10.0）脆弱性应当最先修复，然后修复 CVSS 分值为 9 的脆弱性，直到 CVSS 分值从 4.0 至 10.0 的所有漏洞都被纠正。
4.0 -- 6.9	中危	失败	
0.0 -- 3.9	低危	通过	CVSS 分值从 0.0 至 3.9 的脆弱性是能够通过 ASV 扫描的，但是从安全角度建议（非强制）对这些脆弱性进行修复。

对于 NVD 严重级别与 ASV 扫描结果的对应关系而言会存在一些特殊的情况，以下是需要 ASV 特殊考虑的情况：

- 该脆弱性并没有被 NVD 收录
- ASV 不认同在 NVD 中给出的 CVSS 分值
- 纯粹的拒绝服务（DoS）脆弱性
- 该脆弱性违反 PCI DSS 的要求或者风险级别高于 NVD 的描述

ASV 扫描报告

PCI SSC 对于 ASV 扫描报告格式有严格的要求，每个 ASV 在报告中都需要包含以下的内容：

- 扫描认证的合规性

  这部分的内容是整体的总结，主要显示客户的基础架构是否满足 PCI DSS 审核要求并且通过 ASV 的扫描。

- ASV 扫描报告执行摘要

  这一章节的内容需要列举组件（通过 IP 地址的形式）的脆弱性以显示每个被扫描的 IP 地址是否满足 PCI DSS 审核要求并且通过 ASV 的扫描。这个章节当中，所有的脆弱性都会对应到特定的 IP 地址，每个脆弱性都会与 IP 地址一一对应。

- ASV 扫描报告漏洞详细资料

  这个章节包含对应脆弱性合规的状态（通过 / 失败）的总结以及被发现的脆弱性的详细描述。

除上述描述以外，作为一份被认可的 ASV 扫描报告，它需要包含两个非常重要的元素：被扫描客户对 ASV 扫描的认可声明（包括扫描的范围，客户的信息等内容）另外一个则是具有 PCI SSC ASV 资质认定的人员对于报告的认可。其中最后一个元素被视为 ASV 扫描报告有效性的证明。任何没有经由具有PCI SSC ASV资质认定的人员声明的ASV报告将不被视为一份合规的 ASV 扫描报告。

联系我们

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