atsec information security
Tel: +86-10-82893001
Fax: +86-10-82890017
www.atsec.com

水涨船高，我眼中的外部安全扫描

atsec 王长龙，陈谨运 2012.03

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。

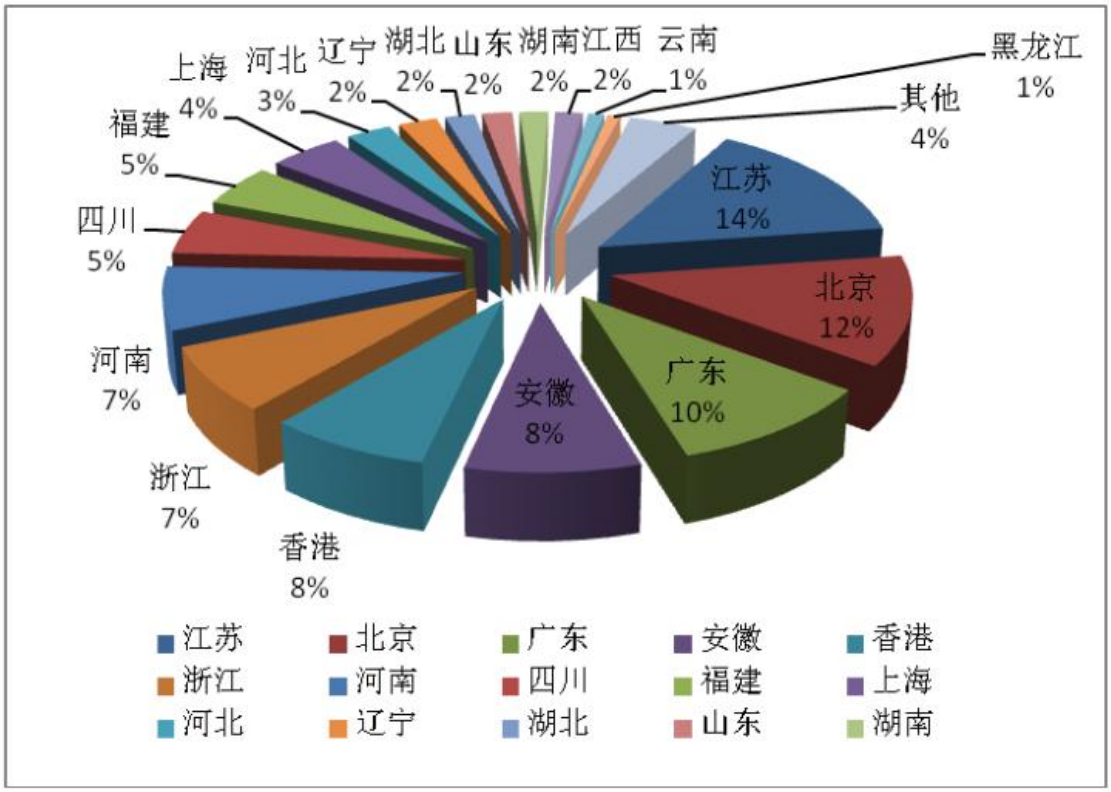
在开始进入正式讨论之前，我们先看两组由中国国家信息安全漏洞库（CNNVD）发布的 2012 年 03 月 05 日至 2012 年 03 月 11 日一周的安全统计数据。第一个图表是对于上述日期内被发现漏洞的类型统计：

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、SQL 注入、跨站脚本、路径遍历、代码注入、信息泄露、跨站伪造请求等等。

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]