安全+
SECURITY
2010/01 总第007
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

探析中小银行信息科技风险管理

从全生命周期构建安全的WEB应用

基线式安全与蝴蝶效应
—论电力信息安全的持续测量、多维保障与运维绩效

WAF vs IPS 谁更适合防护WEB应用?

NSFOCUS

SECURITY

安全+ 技术版
与安全人士分享技术心得
Share technique experience with security professionals

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8668
传真：(010)6872 8708
网址：www.nsfocus.com

2010/01 总第 007

Nsmagazine@nsfocus.com

安全+ SECURITY

© 2010 绿盟科技

本刊图片与文字未经相关版权所有人书面批准，
一概不得以任何形式、方法转载或使用。本刊保留所有版权。

SECURITY 是绿盟科技的注册商标。

需要获取更多信息，请访问WWW.NSFOCUS.COM

目录 CONTENTS

漏洞研究及其成果在运营商系统中的应用

行业营销中心 田民

摘要：从攻击角度上讲，漏洞的发现和利用是入侵者破坏系统最关键的环节。对于防护者来说，现有基于通用漏洞扫描系统的漏洞发现手段，不可避免地存在误报和不能发现未知漏洞的问题。绿盟公司基于对漏洞深入的研究和强大的挖掘能力，为运营商发现了若干严重的系统和业务层面上的漏洞。同时，这些成果已经应用到运营商的安全预警、风险管理以及培训演练等多项工作中，取得了很好的效果。

关键词：漏洞 漏洞发现 漏洞挖掘 漏洞验证 安全预警 攻防演练

引言

运营商重组之后，随着竞争的不断加剧，对业务安全和稳定运营的要求也不断提高。现阶段，三大运营商都已经认识到安全建设对于信息网络、业务以及终端等系统的重要性，制定了丰富的安全规范和安全运维要求，初步建立了一支专业化的安全运维队伍。但是由于运营商的网络系统非常庞大，系统和业务类型非常复杂，系统中存在一些具有较高风险等级安全漏洞的情况很难避免。

近年来，绿盟公司对运营商网络和业务系统进行的大量安全评估服务所得到的报告显示，不管是在支撑网，还是在重要的业务系统中，或多或少存在一些较为严重的安全漏洞，为安全生产埋下巨大的隐患。这些安全漏洞一旦被（内部 / 外部）恶意分子利用而导致安全事故，造成的损失（品牌损失、经济损失等）都是不可估量的。及时发现漏洞以及修复漏洞，防患于未然，在安全事故发生之前就将其扼杀在襁褓之中，对于运营商基层安全运维至关重要。

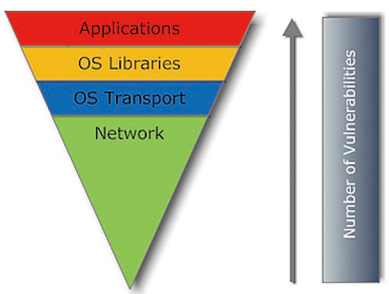
什么是漏洞及其发展趋势

从漏洞的发展趋势来看，应用层面的漏洞远远多于操作系统层面的漏洞。

从软件开发角度上讲，漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误；从业务角度上讲，漏洞是业务在交互处理过程中存在的设计缺陷或逻辑流程上的不合理。这些缺陷、错误或者不合理因素可能被不法者或者黑客利用，诸如通过发送含有恶意代码的数据包方式来攻击或控制整个系统，窃取重要资料，篡改用户信息，进行非法或恶意的订购，或以该系统为跳板入侵其他更为核心的主机系统。

从漏洞的发展趋势来看，应用层面的漏

洞远远多于操作系统层面的漏洞。特别是基于 WEB 应用系统的漏洞更是占据了 80% 以上的已发现漏洞。据此，我们可以得到两个结论：第一，操作系统厂商的软件开发过程越来越完善，可以被利用的软件漏洞越来越少；第二，HTTP/HTTPS 协议具有巨大的发展潜力和应用前景，同时基于 HTTP/HTTPS 协议的应用也逐渐成为黑客关注的焦点。



Source: SANS.ORG

Figure-1 网络、操作系统和应用的漏洞数量

运营商业务系统的漏洞现状

业务漏洞相对于操作系统的漏洞和通用应用的漏洞更为复杂和隐蔽。

在运营商众多而纷杂的系统中，不仅存在操作系统和应用层面（如 WEB 应用）的漏洞，同时存在相当数量业务层面上的漏洞。这些业务漏洞相对于操作系统的漏洞和通用应用的漏洞更为复杂和隐蔽，其产生原因主要归结为以下三种情况：

1) 协议自身的漏洞。

协议自身的漏洞体现在如 GSM 协议、WAP 协议和 SIP 协议等自身存在的漏洞。这些标准化的通信协议或多或少地存在与生俱来的脆弱性，可以被攻击者利用，进行诸如使用虚假主叫号码发送短信，以及利用溢出漏洞发动拒绝服务攻击等行为。

2) 业务流程上的漏洞。

运营商的很多业务系统，在规划和设计阶段，对于业务流程更多地是考虑如何保证业务顺畅的执行，而对安全的考虑不是很全面。很多关键业务系统之间的通信，为了保证其效率，建立了系统间的信任关系，并采用了比较简单的鉴权手段，如基于 IP 地址的认证。其隐患在于攻击者可以利用系统间的信任关系，进行诸如恶意订购等行为。

3) 业务处理的漏洞。

某些核心业务系统，比如计费系统，对于账单文件的内容格式采取了比较严格的规定，但是往往存在对于文件的命名和文件的数量缺乏必要的限制和校验。攻击者通过编造虚假计费账单文件，导致高额话费或零计费事件的发生。

此外，和业务相关的漏洞还包括业务逻辑上的漏洞，如利用业务处理逻辑上的脆弱性，攻击者利用这些漏洞发动绕过认证或计费等目的的攻击。

漏洞发现的意义

漏洞的发现是攻防双方博弈的关键，攻防的双方谁先于对方发现可被利用漏洞，谁就占有战场的制高点，把握到胜利的先机。

对于运营商来说，漏洞、特别是业务漏洞，一旦被恶意攻击者

利用，往往会造成非常严重的经济损失。因此，漏洞的提早发现就显得非常的重要和必要。

无论对于攻击者还是防护者来说，漏洞发现的意义都是非常巨大和关键的。从攻击者的视角上看，漏洞的发现往往是成功入侵和破坏系统的首要环节。分析其攻击路径，漏洞的发现和利用是攻击路径中最重要的步骤，攻击者正是通过不断地尝试寻找这些漏洞，并试图利用这些漏洞控制系统，达到恶意的目的；从防护者的视角上看，如何在漏洞被黑客利用之前发现它并修复它是系统安全防护中非常重要的一项工作。从安全攻防的事前、事中和事后三个阶段来看，漏洞发现和修复是事前防护阶段最主要的安全工作。

因此，漏洞的发现是攻防双方博弈的关键，攻防的双方谁先于对方发现可被利用的漏洞，谁就占有战场的制高点，把握到胜利的先机。作为防守一方的运营商需要尽早发现并修复漏洞。对于业务系统中存在的种种漏洞，如果不能早于攻击者发现，就有可能被攻击者所利用而造成不可弥补的损失。越早发现并修复漏洞，安全防护成本越小，安全事件发生的概率也就越低。

现阶段，漏洞发现主要通过专业的漏洞扫描系统来实现。漏洞一旦被公布，在第一时间通过漏洞扫描系统检测业务系统中是否存在类似的漏洞以及快速修复漏洞，是解决此类漏洞最有效的方式和方法。

漏洞发现工作中存在的问题

由于漏洞扫描系统自身的技术实现原理，或多或少存在扫描误报的问题，同时，通用漏洞扫描系统对于专有业务系统业务漏洞的发现几乎无能为力。

在运营商的安全运维中，对于已经公布的漏洞，主要依托专业的漏洞扫描系统来发现。漏洞扫描系统是一种能自动发现远程服务器端口分配和判断所提供服务，并检测远程或本地主机安全弱点的系统。通过使用漏洞扫描系统，系统管理员能够发现所维护服务器的各种 TCP 端口分配、提供的服务、服务软件版本和这些服务及软件上的安全漏洞。

漏洞扫描系统对维护人员及时发现系统漏洞提供了便利，自动化的操作极大地简化了漏洞发现的流程。然而，从另一个角度上讲，由于漏洞扫描系统自身的技术实现原理，或多或少存在扫描误报的问题，使得系统管理员对漏洞的真实性无法评估。同时，漏洞扫描系统客观存在的功能局限性也使得使用者对漏洞的实际危害性缺乏必要的判断手段。

这些因素将直接影响到对漏洞修复的决策。特别是关键业务系统上的高危漏洞，一方面，担心漏洞扫描系统误报，不知道漏洞是否真实存在；另一方面，对漏洞实际的危害性不得而知，威胁程度不能直观地体现出来。

此外，相对于已公布的操作系统和通用应用系统的漏洞，大量专有业务系统以及定制化业务系统存在的应用和业务层面的未知漏洞，对于业务正常运营的安全威胁就显得更为隐蔽和严峻。这些未知的安全漏洞可能造成的安全损失，相对于操作系统漏洞，可能更为严重，破坏性更为巨大。

通用漏洞扫描系统对于发现这些未知漏洞，特别是专有业务系

统的业务漏洞几乎无能为力。发现这些未知漏洞，一方面依靠业务系统厂商公布的系统漏洞，另一方面依靠手工的漏洞挖掘。然而，业务系统厂商公布的漏洞主要集中在系统层面，应用和业务漏洞少之又少；同时，对于运营商的系统管理员和安全管理员来说，虽然对业务系统非常了解，但是受到其对安全攻防的理解以及渗透技能的限制，很难依靠自身能力对业务系统进行未知漏洞的挖掘。

如何解决漏洞发现中的问题

漏洞验证最主要的目的是检验漏洞扫描结果的准确性；同时，对于未知漏洞、特别是业务漏洞的发现，可以依托安全专家通过漏洞挖掘工作来实现。

对于漏洞发现过程中存在的上述问题，可以归结为两大类：

1、漏洞扫描系统准确性（主要是误报）以及威胁无法呈现的问题；

2、未知安全漏洞，特别是业务漏洞的发现问题。

首先，对于影响漏洞修复决策的漏洞扫描结果不准确和无法直观呈现漏洞威胁程度的问题，比较可行的办法是对发现的漏洞进行验证。

漏洞验证的原理是通过在可触发系统漏洞的数据包上注入预先定义的 shellcode 代码（一段攻击性代码），该代码触发系统中存在的漏洞。比如用于在溢出后改变系统正常流程，从而完成诸如执行目标主机上的系统指令等攻击目标。

漏洞验证有自动验证和手动验证两种方式。自动验证是通过调用攻击代码（shellcode）对漏洞进行自动化验证，攻击的交互过程不需要人工干预，验证的效果可以在系统中直观地显现出来；然而，绝大部分漏洞的验证需要手工进行。手工漏洞验证需要事先制定验证方案，遵照一定的步骤和流程，通过调用相应的工具和测试用例，由安全人员对目标系统进行逐步地渗透和漏洞验证。

由此可见，漏洞验证本身也是一种漏洞利用的过程，是模拟攻击者对存在漏洞的目标系统发起攻击，并利用存在的漏洞实现控制目标系统，实现一定入侵目的的行为。从另一个角度上讲，对于防护者来说，漏洞验证不失为一种检验漏洞是否真实存在及其对危害性进行评估的有效手段。

漏洞验证最主要的目的是检验漏洞扫描结果的准确性。通过漏洞扫描系统发现的漏洞，只要可以验证并成功验证，就一定是真实存在的漏洞，同时也是未来可能被攻击者所利用的漏洞；另一个目的是通过模拟攻击者入侵的方式直观地将漏洞的危害展现出来，在很大程度上重现攻击者利用漏洞破坏系统而导致的直接后果。

对于未知漏洞、特别是业务漏洞的发现，可以依托安全专家通过漏洞挖掘工作来实现。对于不同的业务系统，不同的安全专家所采取的漏洞挖掘方法也是不同的。

业务漏洞的发现对漏洞挖掘人员的要求是很高的。不仅要求挖掘人员对安全攻防具有深刻的理解和较高的代码编程技能，同时也要求其必须了解目标系统的业务流程。一般来说，对运营商专有业务系统漏洞的挖掘工作由安全专家主导，系统管理人员和系统开发厂商的技术人员配合，共同完成业务漏洞的挖掘工作。除了对人员组成的要求之外，对系统环境的要求也较高。测试环境越接近现网系统，挖掘出来的漏洞成果就越真实和具有代表性。

漏洞研究成果在运营商系统中的应用

绿盟配合国内运营商对业务系统进行了多次深入地漏洞挖掘，发现了若干严重的系统和业务层面上的漏洞。这些成果已经应用到安全预警、风险管理以及培训演练等多项工作中，取得了很好的效果。

近年来，绿盟公司依托强大的漏洞研究和挖掘能力，为微软、思科等厂商发现近40个严重的安全漏洞。同时，绿盟配合国内运营商对其业务系统进行了多次深入的漏洞挖掘。这些成果涵盖了从系统层面到应用层面以及业务层面，包括针对专有业务协议的拒绝服务类漏洞，嵌入式业务终端的溢出漏洞，以及计费过程中的业务处理漏洞等。在安全漏洞的发现和防护工作上，绿盟公司帮助运营商先于攻击者发现并修复漏洞，实现了防患于未然的目的，作出了力所能及的贡献。

与此同时，考虑到运营商基层运维人员对业务漏洞及其危害作用普遍缺乏直观的了解，本着提高运维队伍自身的安全意识和技能水平，掌握一定的安全评估、特别是渗透测试能力，以及建立统一管理和共享的脆弱性知识库为目的，绿盟配合运营商开发了安全预警、风险管理和攻防培训演练的系统和平台。

基于平台，运维人员可以查询相关数据业务系统存在的漏洞，调用平台所携带的漏洞扫描和漏洞攻击验证模块，切身体验黑客入侵的过程以及直观感受到漏洞利用导致的危害。在了解攻击过程及其危害的基础上，平台对于漏洞的修复提供具体建议，指导运维人员进行系统加固。

参考资料

[1] SANS.ORG. The Top Cyber Security Risks. http://www.sans.org/top-cyber-security-risks/.

[2] Michael S. Minoso. Cybersecurity's profile rising under Obama. 2009 年 3 月 . http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349663_mem1,00.html.

[3] 单国栋，戴英侠，王航 . 计算机漏洞分类研究 [J]. 计算机工程，2002，（10）:1-2.

安全，提升IDC竞争力

行业营销中心 万慧星

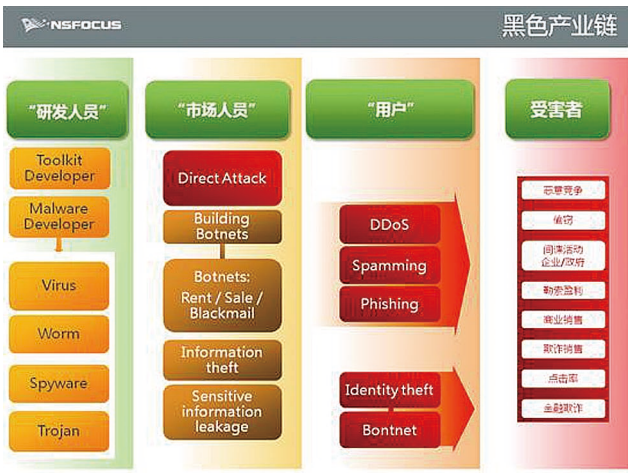
IDC 现状概述

大家都知道，IDC 是互联网的基础设施，承载着大量的互联网资源，是互联网的数据中心，更是所有运营商的必争之地。而作为正处于移动互联网转型的中国移动，不论是 3G 业务的大规模发展，还是提高个人用户上网访问速度，增加上网体验，都需要 IDC 的内容作为支撑；而对于争夺集团客户和进行移动互联网的业务转型，也都离不开 IDC。因此，对于现阶段的中国移动来说，IDC 就显得更为重要。

众所周知，由于历史原因，互联网和 IDC 业务一直是中国电信和中国联通的传统优势项目。基于移动互联网战略需求，当前中国移动正在进行大规模的 IDC 布点和建设。如何充分利用后发优势，提供差异化的竞争就成为了关键。从“一点接入，全网服务”架构的提出，到“CDN、虚拟化计算”等技术的引入都为差异化服务提供了基础。同时，基于对 IDC 安全的研究，绿盟科技认为 IDC 的安全也将是构建差异化服务的关键。

换一个视角看 IDC 安全

近几年，在 IDC 高速发展的同时，IDC 中发生的安全事件也越来越多，面临的安全威胁也越来越严峻。常见的安全事件主要有：大规模的攻击流量严重地侵占了 IDC 的出口带宽，降低了 IDC 整体服务的可用性；内部大规模的蠕虫病毒爆发，被感染的服务器发送大量的 UDP 数据包，形成 UDP Flood，造成的 IDC 内网络拥塞甚至瘫痪；虚拟主机受攻击，致使整台虚拟主机受影响，而虚拟主机中的所有用户虚拟 WEB 服务器也无法提供服务；2009 年初开展的“整治低俗之风活动”，一些未备案注册网站、一些存在低俗信息的网站，陆续被曝光和要求整改，而 IDC 作为互联网信息的集散地和接入单位，往往也受到牵连。

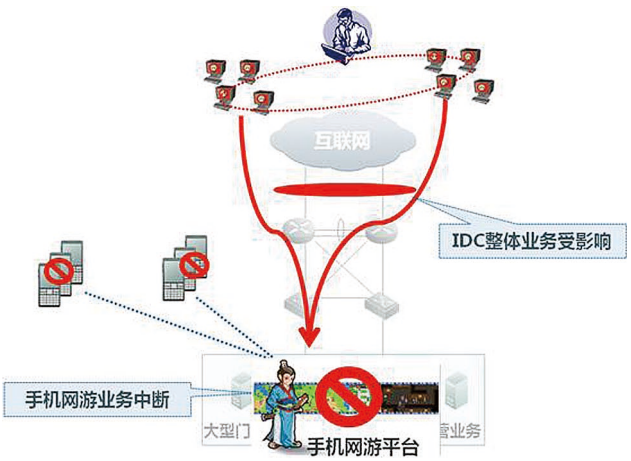


黑色产业链示意图

在这些安全事件的背后，还有一条看不见的链条——黑色产业链。在这条产业链中，有人专门负责进行研发——漏洞挖掘和利用工具的编写；专人进行产品的开发——利用漏洞和工具进行僵尸网络的发展，开发攻击的“炮弹”；有人再将这些产品或租或售提供给恶意使用者对目标发起攻击，实现对恶意竞争、信息偷窃、间谍活动等等，导致目标系统的价值损失。IDC 作为互联网内容的集散地，是各种攻击最为密集的地方，使 IDC 成为了受害的重灾区；同时，由于 IDC 中的服务器受黑客控制，最终也可能致使 IDC 成为了攻击发起的平台。

IDC 面临的主要安全挑战：

安全挑战一，DDoS 攻击，影响 IDC 网络可用性



对于 IDC 中托管的主机来说，不论是自营业务还是托管业务，最基本的应用就是需要满足互联网用户的访问需求，也就是说可用性是 IDC 客户最为看重的安全特性，而 DDoS 带来的主要挑战就是影响了可用性，因此对于 IDC 来说是最为严重的安全威胁。

一个典型案例，手机网游是 3G 业务中，用户黏度非常高的一种业务应用。随着用户规模的扩大，网游系统也越来越受到竞争对手的关注，有可能受到竞争对手发起的恶意竞争——针对网游平台发起 DDoS 攻击。DDoS 攻击通常由网络中的僵尸主机发起，通过大量的非正常访问，致使网游平台资源越来越紧张，直至不能提供正常业务。随着攻击的持续，流量逐渐增大，造成 IDC 边界带宽也受到阻塞，最终有可能造成整个 IDC 业务受影响。

安全挑战二，弹药库，影响 IDC 内部网络或者冲击互联网资源

IDC 像一个弹药库。由于 IDC 中的高性能服务器、高端网络设备，高带宽连接互联网，使 IDC 成为了一个威力强大的“弹药库”。这个“弹药库”有可能内部发生爆炸影响 IDC 的服务质量；也有可能被恶意使用，冲击互联网资源，对运营商的基础设施造成影响。

IDC 由于自身内部结构复杂，各自系统的安全状况大不相同。一方面，IDC 中一些安全防护薄弱服务器系统，有可能被感染蠕虫病毒，感染后的服务器发送大量的数据包，形成网络蠕虫风暴，使网络性能急剧下降，造成 IDC 内部网络效率降低，影响了 IDC 的可用性。另一方面，由于黑色产业链的工作，IDC 中一些安全防护较薄弱的服务器，有可能被发展成为僵尸网络的节点，黑客可以控制这些节点对互联网的其他站点发动攻击，冲击互联网资源，最终可能致使 IDC 的 IP 地址被列入“黑名单”。

安全挑战三，针对 WEB 应用的攻击，IDC 客户最为关心的安全问题

据统计 IDC 中对互联网提供服务的站点，超过 80% 都是基于 WEB 的应用业务，当前针对 WEB 的安全攻击已经越来越频繁，而且攻击类型多种多样。通常来看，基于 WEB 应用的安全攻击可分为两类：一是利用 WEB 服务器的漏洞进行攻击，如 CGI 缓冲区溢出、目录遍历漏洞利用等攻击；二是利用网页自身的安全漏洞进行攻击，如 SQL 注入、跨站脚本攻击等。基于上述攻击，可导致网页篡改、网页挂马、信息窃取等网站安全事件的产生，给网站造成很大的威胁。对于 IDC 中的业务站点来说，一旦 WEB 受到攻击或者破坏，也就直接影响了网站的正常运行。由于 IDC 中 WEB 站点众多，如何防止 WEB 站点受到攻击，提高 IDC 中 WEB 站点的安全防护，将成为 IDC 的一个竞争优势点。

安全挑战四，内容层面的安全威胁，带给 IDC 极大的政治和法律风险

自“整治低俗之风专项行动”开展以来，IDC 中未备案网站、存在低俗信息的网站，陆续被曝光和要求整改，而 IDC 作为网站的集散地和接入单位，往往也受到影响。对于未备案网站的发现，第一步就是需要掌握 IDC 中存在了哪些域名，但由于 IDC 中二级代理、虚拟主机等实际情况的存在，使 IDC 的运维管理人员很难通过入网登记的业务流程来掌握 IDC 中的域名信息；对于不良信息在 IDC 中长期存在的事实，IDC 很难依靠现有的技术手段，对网站中存在的低俗信息进行有效的监控。这些都可能给 IDC 带来极大的政治和法律风险。

综上所述，IDC 对中国移动具有非常重要的战略价值，但由于各种安全挑战的存在，可能会导致 IDC 价值的破坏和损失。因此，需要对 IDC 的安全问题进行有效的处理，降低安全风险，并通过安全来提高行业竞争力。

安全！提升 IDC 竞争力

安全问题发生的主要原因

传统的 IDC 安全防护特点：

1. 重视外部防护，忽视内部安全。传统 IDC 安全防护更看重对外部防护，比如在 IDC 的边界部署防火墙等手段进行边界防护，但 IDC 内部就任由网络互联互通，没有任何的防护措施，致使内部的蠕虫病毒爆发无法阻挡。

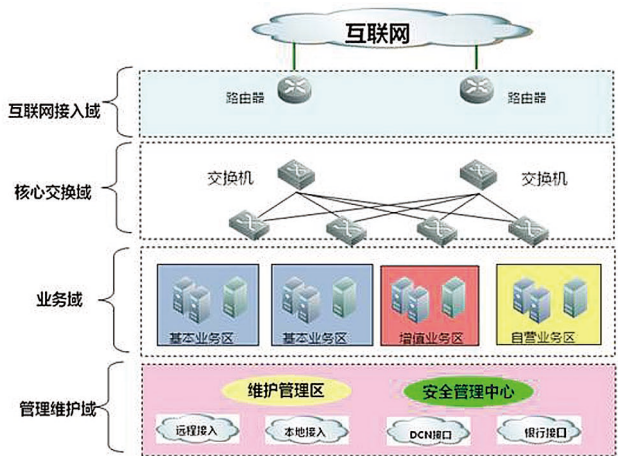
2. 安全防护不分区。不论是针对自营业务还是托管业务，也不管是普通的 WEB 托管站点，还是 VIP 站点，都将其部署在一个业务区域，服务等级也相似。

3. 重视网络层防护，忽略了应用于内容层面的安全。当前应用层的攻击越来越多，传统网络层的防护措施显得无能为力，防护效果也无从谈起。

安全保障，提升 IDC 竞争力

安全建设有很多内容，但并非是考虑全面了就不会再出现安全问题，我们本着适度安全的观点出发，仅针对 IDC 面临的主要问题提建设思路。（如想进一步了解 IDC 的建设方案可以参考绿盟科技的 IDC 安全解决方案）

1. 搭建基础架构



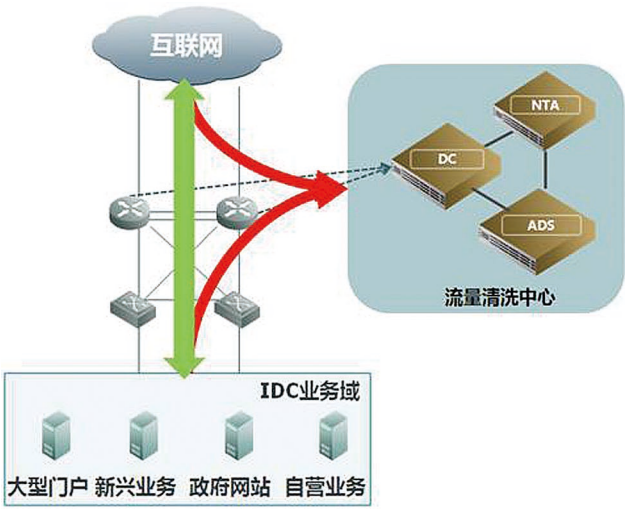
IDC 安全域划分示意图

安全域。搭建一个安全架构，根据业务的不同对 IDC 进行安全域的划分，可以划分为互联网接入域、核心交换域、业务域、维护管理域等不同业务功能的安全域，使复杂的网络结构简单化，再针对这些业务实现不同强度的安全保护，更好的保障网络上承载的业务。

边界控制。有了安全域的划分基础，下一步就是对各个区域进行隔离，实施边界控制，防止“交叉感染”。对于安全域的边界控制，可以采用划分 VLAN、MPLS VPN 通道，以及防火墙等手段进行。根据 IDC 的实际情况，通常来说对于 IDC 内部区域之间的隔离和边界控制，采用划分 VLAN，然后采用 ACL 进行控制，对于整个 IDC 域外部网络的边界则采用防火墙来实现。

安全基线。通过边界控制，有效地防止了“交叉感染”，现在还需要从系统、设备自身安全出发，降低系统层面的安全风险。系统自身安全从安全漏洞、安全配置，以及异常服务等 3 个维度出发，对系统进行安全加固。对于 IDC 客户托管系统，难于强制进行安全基线加固，可采用在客户托管系统的业务域边界进行严格限制，防止安全隐患影响其他区域。

2.DDoS 攻击防护



IDC 流量清洗示意图

根据对 IDC 面临安全挑战的分析，DDoS 攻击是 IDC 可用性最大的安全威胁，攻击给 IDC 客户带来影响的同时也给 IDC 整体的可用性造成影响，因此需要进行重点防范。对于 DDoS 防护，需要与骨干网整体 DDoS 流量清洗防护体系相结合，实现多层立体防护。同时，IDC 既有可能面对外部的 DDoS 攻击，也有可能成为一个对外攻击的发起平台，因此进行 DDoS 流量清洗还需要考虑双向防护的特性。

3.WEB 应用安全防护

从 WEB 应用的生命周期来看，分为开发阶段、部署阶段、运营阶段等 3 个部分，在不同阶段可以采用不同的安全防护手段。对于 IDC 中上线的 WEB 站点，通常为已经开发完成、正式运行的业务站点，因此 IDC 提供的防护内容也应该重点关注在运营阶段的安全防护。

在运营阶段，防护的关键是能及时地发现针对 WEB 应用的攻击行为，并进行有效的阻断，防止对网站的正常运营造成影响。而传统的防护手段难于对 WEB 应用层的攻击进行检测与防护，因此可以考虑采用 WEB 应用防火墙对其进行专项防护。WEB 应用防护为 IDC 客户提供差异化的安全服务，提升行业竞争力。

4. 不良信息监控

对于 IDC 中的内容安全，需要重点关注到两类站点，一类是对互联网和移动互联网用户提供服务的 WEB 站点，另一类是专门针对移动互联网提供服务的 WAP 站点。需要对这些站点中可能存在的不良信息，及时地发现和控制，防止移动互联网和互联网用户访问。

对于文字、图片等方面的内容信息的识别，当前有比较成熟的解决方案实现。通过在 IDC 的边界旁路部署技术手段，对进出 IDC 的数据流进行检测，发现不良信息。同时，考虑到当前的技术手段还无法实现内容识别 100% 的准确性，因此不建议进行自动化的阻断，而是通过人工复查的方式进行处理。

安全业务，提升 IDC 竞争力

在 IDC 安全建设的基础上，传统的 IDC 越来越多地开始提供安全增值业务，而且取得了不错的效果。安全增值业务的产品很多，主要包括有：

预防类业务：安全预警、安全评估、安全加固、安全巡检等

检测类业务：业务流量分析、异常流量监测、攻击入侵监测等

控制类业务：应急处理、攻击阻断、异常流量清洗、蠕虫病毒控制等

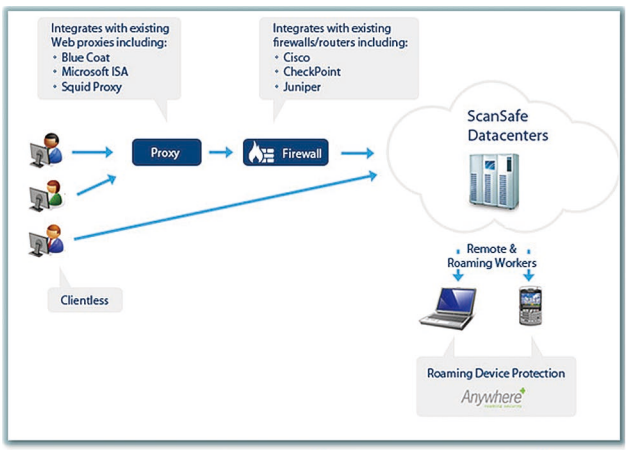
补偿类业务：日志分析、攻击取证、业务应急恢复等

从实际推广的效果来看，IDC 客户对 DDoS 攻击流量检测与清洗的安全增值业务接受程度较高。DDoS 清洗业务以自动化流量检测和清洗工具为基础，对 IDC 的运维人员要求较低，可以完全实现自动化。通常为客户提供包月计费与按次计费两种模式。在绿盟科技与 IDC 合作的一个安全增值业务案例中，DDoS 流量清洗业务直接为 IDC 带来了 5% 的业务收益和 20% 的业务增长，在当地树立了安全 IDC 的品牌，对互联网企业和电子商务网站的吸引力颇大。

在安全增值业务开展的过程中，我们对政府、企业、互联网企

业等 IDC 的重点客户进行调查，分析发现客户普遍存在网站专项防护、应用加速和来访数据分析等方面的增值业务需求。这些业务还没有在 IDC 中大规模的展开，因此可以将其纳入到 IDC 的安全增值业务中，为客户提供差异化的安全增值服务，提高行业竞争力，同时也提高业务收益。

IDC 安全的未来



Source:www.scansafe.com

云计算是大家所看到的 IDC 重要发展方向，云计算可以利用 IDC 中大量的计算资源为个人、中小企业用户提供更为丰富的业务应用，同时，在云中引入虚拟化技术，可以有效地降低能耗，促进节能减排。而在云的应用方面，我们已经看到云安全就是云计算的一种很好的应用方向。

通过云安全的特性提高病毒查杀的效率和准确性，云安全不是某项新产品，也不是解决方案，它是基于云计算技术演变而来的一种互联网安全防御理念。当前来看，国内对于云安全领域的涉足，主要以防病毒厂商为主，提供的主要服务内容还是与病毒防治有关，其实云安全作为一个平台，还可以提供非常广泛的应用。

我们一起来看一下，基于云安全平台为企业和个人客户提供安全服务的一些应用。ScanSafe 运用云安全平台提供 SaaS 模式的安全服务，包括 WEB Security、WEB Filtering、Anywhere+ 等，针对用户的 WEB 访问提供实时的扫描和控制。通过 ScanSafe 的云安全服务，用户无论是处于固定位置还是处于移动状态，只要连接了互联网，都可以享受同样的安全防控级别，而服务对象既包括 PC 用户，也包括智能终端用户。

绿盟科技正在积极地进行云安全的研究和平台建设，现阶段已经推出了基于云平台的 WEB 站点安全检查服务，主要核心是基于互联网信誉系统。信誉系统从众多信息来源获取的互联网安全相关数据，在分析和关联后形成互联网信誉库。 针对近期广受关注的“整治互联网低俗之风”、“手机涉黄”等事件，应用信誉系统掌握存在可疑信息的站点，一方面为运营单位和主管机构控制源头提供数据；另一方面也可以作为个人用户互联网访问的一个控制列表，提高用户的互联网访问安全性。

由于中国拥有广泛的互联网和移动互联网用户，如何利用 IDC 的计算资源，开启云安全服务，为广大的移动互联网用户提供安全服务，开拓广阔安全市场空间 ，值得我们深入探讨。

探析中小银行信息科技风险管理

行业技术部 徐一丁

摘要：2009 年 3 月 3 日，银监会发布了《商业银行信息科技风险管理指引》（以下简称“新《指引》”），标志着银行业信息安全建设进入了新的阶段。绿盟科技根据新《指引》，为几家中小银行客户提供了管理咨询服务，其中包括农信联社、区域性（省级 / 市级）银行。在本文中，我们将相关工作中的经验与思考进行分享。

关键词：新《指引》 信息科技风险 信息安全 中小银行

新《指引》与银行业信息科技风险监管

银监会在 2006 年发布了《银行业金融机构信息系统风险管理指引》，标志着全行业 IT 相关的风险管理工作正式开展，同期发布的《关于开展 2006 年度信息科技风险内部和外部评价审计的通知》（313 号文）及其附件，是银行进行具体审计工作的指导性文件。全国相关的银行机构据此进行了 IT 系统风险的内审与外审工作，并将结果上报到银监会。

2009 年 3 月，银监会发布了新一版的指引，并将其名称变更为《商业银行信息科技风险管理指引》，银行业信息科技风险管理工作进入了新的阶段。

新《指引》的发布，将对我国银行业信息科技风险管理产生积极作用。首先，新《指引》规定了董事会和高级管理层在信息科技风险管理中承担的主要责任，提出要构建信息科技风险管理的“三道防线”（即信息科技管理、信息科技风险管理、信息科技风险审计），要求商业银行在决策层设立首席信息官，有利于商业银行加强信息科技治理；其次，新《指引》对商业银行在具体操作层面提供了可供借鉴、操作性强的较高要求，有利于促进商业银行信息科技风险管理水平的持续提升；另外，对敏感信息保护要求的提出，特别是对外包服务环节信息保护的要求，将促使商业银行进一步加强客户信息保护，为广大储户提供更加安全的服务。

中小银行现状与新《指引》的差距

从我们了解的实际状况看，中小银行与监管部门的要求普遍存在差距，主要表现在以下方面：

信息科技风险与信息安全的关系未理清

2006 年的《银行业金融机构信息系统风险管理指引》名为“信息系统风险管理”，实质上已经为“信息科技风险管理”打下了基础。随着行业内内审、外审的推进，监管部门在后续工作中已经逐步将“信息科技风险”的概念清晰化，并在新《指引》中明确提出，作为银行整体风险的一部分来看待。

而国内中小银行普遍还未紧跟监管部门的思路。信息安全还是信息安全，归 IT 部门管；风险管理还是风险管理，归风险管理部门管。两个部门工作间没有交互，信息科技风险没有在银行整体风险中体现，这显然不符合新《指引》的要求。

岗位设置不符合要求

随着新《指引》的出台，监管部门已经明确了“信息科技管理、信息科技风险管理、信

息科技风险审计”的三道防线，这些工作已经远远不是 IT 部门能够承载的。商业银行普遍没有设立信息科技管理委员会，在风险管理部门和稽核审计部门也没有专业的 IT 人员。

“不在其位，不谋其政”。没有相应的内部机构和岗位，从长期看会导致银行相关工作无法推进与落实，信息科技风险管理、审计的专业经验无法积累，水平也无法提高。

信息安全管理不成体系

中小银行通常在信息安全管理方面已经有很多可执行的管理办法、指引、制度，并制定了流程，能够基本支撑日常的业务运营，但这些制度并没有按照合理的框架去梳理归纳。这直接导致了制度之间的层级、关系不明确，可能造成某些重要制度的缺失，也可能使一些制度内容重复，在实施时面临多个指导，使效率降低或操作错误。

信息安全被认为是“IT 部门的事”，没有落实到每个部门

银行整体层面缺乏对信息安全的正确认识。认为安全管理只与 IT 部门相关，没有意识到自己在信息安全中的作用与责任。如自己的办公 PC 闹病毒，只是让 IT 人员来杀毒，问题解决后不吸取教训，仍然随意访问不明网站，收发 e-mail 也不加检查，过几天病毒又发作等等，信息安全没有内部全员参与，这样做致使 IT 部门的工作成本高，也达不到应有的安全水平。

信息科技风险管理改进

建议改进工作按照“摸清情况，合理规划，分步实施”的思路进行。国内中小银行与新《指引》的要求普遍有较大的差距，想要去弥补就不是一朝一夕的事情。监管部门也会尊重客观规律，不会强制各银行马上就达到要求。但我们应重视新《指引》，切实展开相关的工作。可以根据新《指引》的要求对比自身情况，做出差距分析，并制订整改规划。规划可能是两年、三年或五年期的，然后再根据轻重缓急，将其拆分为每年、每季度的执行方案，分步进行建设。

进行相关改进的时候，建议注意以下要点：

信息科技风险应纳入银行整体风险管理体系

信息科技风险是操作风险的一部分，通过操作风险的管理纳入到银行整体风险管理体系中。信息安全是信息科技风险管理中核心且关键的内容，很多信息科技风险管理的操作会基于信息安全管理来进行。

根据情况进行组织调整

根据新《指引》内容，银行应有信息科技管理委员会、CIO、信息科技风险管理、信息安全管理和信息科技审计等机构和岗位。银行可以根据这些要求，结合自身组织情况来逐步建立和调整。组织调整不可不做，也不可操之过急，否则会对业务运营产生负面影响。

建立完善的信息科技风险 / 信息安全管理体系，贯彻到全行

银行根据自身情况搭建起适合的信息科技风险管理体系，分层次进行设计，如由上至下分为“方针策略、体系维护、规范制度、操作执行”等四层。供具体操作的 IT 相关规范制度，银行一般都有，可以将现有的这些文档进行筛选、调整后，填充到新体系中去。这样既省时省力，又可以保证体系可落地执行。根据情况，应该还需要编写一部分新的管理制度文档。

信息安全的管理由 IT 部门负责，而执

行需要在全行每个部门和岗位落地。IT 部门要为全行建立基础的信息安全策略、制度，组织安全意识培训、帮助部门设立安全岗位，并提供必要的安全技术支持。在此基础上，全行的业务、行政、财务、后勤等各个部门都应切实地参与进来，在完成本职工作的同时，严格遵循信息安全管理的规定，保证自己这里不出问题。

配合监管部门的检查

据了解，银监会下发了新《指引》之后，也在内部组织编写了相关的现场检查指导手册，各地银监局会以手册为依据，对所辖片区内的银行进行现场检查。根据新《指引》内容来判断，监管部门的现场检查可能包括文档审查、人员访谈、现场勘查、技术检测等手段，视现场时间的长短，检查的细致程度会有所不同。

银行应积极配合监管部门的检查，借助监管部门的工作来找出自身的问题，并妥善进行处置。从风险管理的原理来说，评估、审计、检查都不是目的，而是通过这一系列的活动，来达到充分识别风险和有效管理风险的目标。

参考资料

[1]《商业银行信息科技风险管理指引》

[2] 银监会相关负责人就《商业银行信息科技风险管理指引》答记者问

[3]《银行业金融机构信息系统风险管理指引》

[4]《关于开展 2006 年度信息科技风险内部和外部评价审计的通知》

[5]《2006 年度银行业金融机构信息科技风险评价审计要点》

绿盟科技与银行业

绿盟科技（NSFOCUS Co., Ltd.）从 2000 年成立迄今，已经为国内 56 家银行客户提供了专业服务与安全产品，客户包括中国人民银行、中国银监会、五家国有大型银行、三家政策性银行、部分全国性股份制商业银行和区域性商业银行，另外还有外汇交易中心、银联等业内重点机构。

绿盟科技通过专业的服务与产品赢得了银行客户的普遍信任。信任既是压力也是动力，我们会继续做好“巨人背后的安全专家”，一如既往地为银行业服务，为中国金融事业的稳定和持续发展尽自己的一份力量。

从全生命周期构建安全的WEB应用

产品市场部 李晨

摘要：本文从WEB 应用现状及威胁分析入手，阐明 WEB 应用目前面临的挑战。通过对绿盟远程安全评估系统的功能特性介绍，详细描述如何利用该系统协助政企机构制定全生命周期的 WEB 应用安全解决方案，为 WEB 应用保驾护航。

关键词：WEB 应用 风险管理 漏洞扫描 威胁

1. 引言

随着 WEB 应用的普及，政府机构和企业都竞相部署了 WEB 应用系统作为信息发布的窗口。同时更多的对外业务也越来越多地转向 WEB 平台上，如网上办公，网上营业厅等。WEB 应用的发展及蕴藏信息价值的提升，必然引发黑客的攻击热潮，近两年来各类 WEB 应用安全事件层出不穷，如网页篡改、信息泄露、网站挂马等。

如何保证 WEB 应用整个生命周期的安全性？如何发现组成 WEB 应用的各层结构的隐藏安全漏洞？如何将安全风险控制点前移，做到事前修补安全漏洞从而未雨绸缪？

本文从 WEB 应用现状及威胁分析入手，阐明 WEB 应用目前面临的挑战。通过对绿盟远程安全评估系统的功能特性介绍，详细描述如何利用该系统协助政企机构制定全生命周期的 WEB 应用安全解决方案，为政企单位的 WEB 应用保驾护航。

2.WEB 应用现状与威胁

2.1 WEB 应用体系架构

要对 WEB 系统提供安全防护，必须了解 WEB 基础架构。一个完整的 WEB 体系架构，通常由四部分构成。

首先客户端是第一部分 ;WEB 服务以及相关实现具体应用的部分属于中间层 ; 后台数据库是第三层，而后台操作系统及网络则对 WEB 应用进行承载和支撑。浏览器端和服务器通过技术平台交换信息数据，在整个 WEB 体系技术平台之上承载的是信息数据。用户通过 WEB 浏览器发送请求给 WEB 服务器，由 WEB 服务将用户的请求转换为对后台数据的查询、提交或是更新，并将最终的结果（信

息数据）在浏览器上展示给用户，而所有的信息数据由 WEB 应用的后台承载系统进行承载和传输。

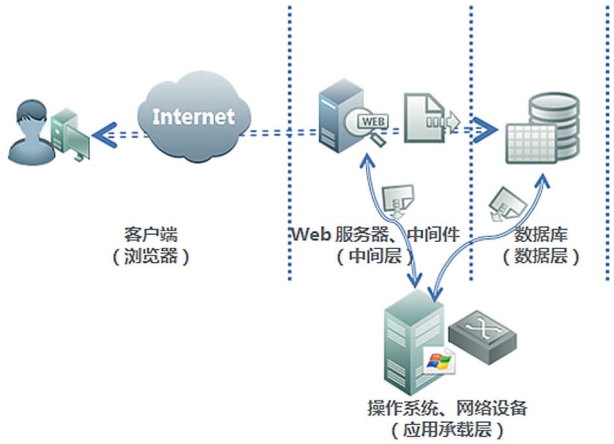


图 1.1　WEB 应用架构图

2.3 WEB 应用威胁

在 WEB 体系架构中，信息层面的安全威胁主要来自于虚假信息、非法信息、信息失密等，我们经常听到的网络谣言、挂马站点、网络钓鱼、泄密等都属于此类型的安全威胁的具体形式。而在技术层面，技术体系中包含的操作系统、浏览器、一般服务组件、网络平台层次所面临的安全威胁都是常见的安全威胁，包括恶意代码（病毒、蠕虫、流氓软件等）、注入攻击、暴力破解、拒绝服务等。威胁和影响如下图所示：

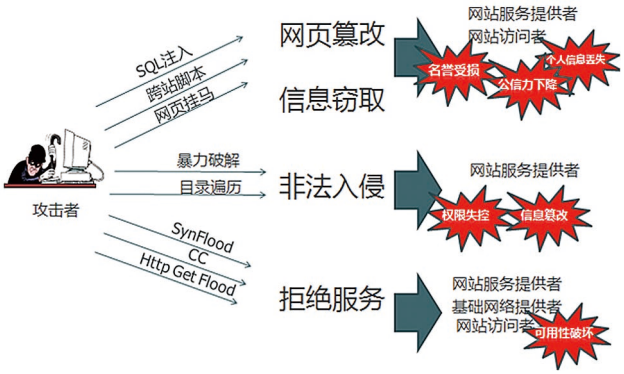


图 1.2 WEB 应用遭受的威胁

通过良好的系统部署、运维策略，结合一些必要的技术手段，就能较大限度地降低安全威胁的影响。目前在整个 WEB 体系的安全威胁中，利用应用系统的安全漏洞进行的破坏是所有安全威胁中占比例最大的一部分。在 OWASP 统计的 2007 年 WEB 应用面临的最常见的攻击行为如下图：

（针对详细攻击方式的描述请参考 http://www.owasp.org/index.php/Main_Page）

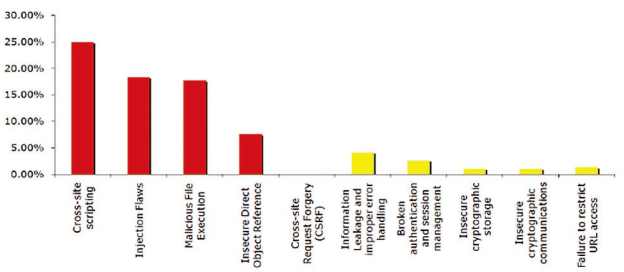


图 1.3 OWASP Top 10 WEB 应用漏洞

2.2 WEB 应用防护体系

在 WEB 应用的各个层面，都会使用不同的技术来确保安全性。首先为了保护客户端机器的安全，用户会安装防病毒软件；为了保证数据传输的机密性，通信层通常会使用 SSL（安全套接层）技术加密数据；同时会使用防火墙和 IDS（入侵诊断系统）/IPS（入侵防御系统）来进行安全防护，屏蔽不需要的端口和控制非法的访问；另外还会使用身份认证机制授权用户的访问行为。

但是，即便有防病毒保护、防火墙和 IDS/IPS，企业仍然不得不允许一部分的通讯经过防火墙，毕竟 WEB 应用的目的是为用户提供服务，保护措施可以关闭不必要暴露的端口，但是 WEB 应用必须的 80 和 443 端口，是一定要开放的。经过这部分的通讯，可能是善意的，也可能是恶意的，很难辨别。同时，由于 WEB 应用是由软件构成的，那么它一定会包含缺陷（bugs），这些 bugs 就可以被恶意的用户利用，他们通过执行各种恶意的操作，或者偷窃、或者操控、或者破坏 WEB 应用中的重要信息。

■ 因此可以看出，纯粹在 WEB 应用上线后的安全防护措施，并不能真正保证企业的应用安全：

■ 防火墙可以阻止对重要端口的访问，但是 80 和 443 端口始终要开放，我们无法判断这两个端口中通讯数据是善意的访问还是恶意的攻击；

■ IDS 可以监测常规的攻击事件，但是对于变形攻击和 0day 攻击，无法进行有效的监测；

■ SSL 可以加密数据，但是它仅仅保护了在传输过程中数据的安全性，并没有保护 WEB 应用本身；

■ 每个季度的渗透测试，无法满足处于不断变更之中的应用。

只要访问可以顺利通过企业的防火墙，WEB 应用就毫无保留地呈现在用户面前。只有加强 WEB 应用自身的安全，通过对特定 WEB 应用全生命周期的风险管控，才是真正的 WEB 应用安全解决之道。

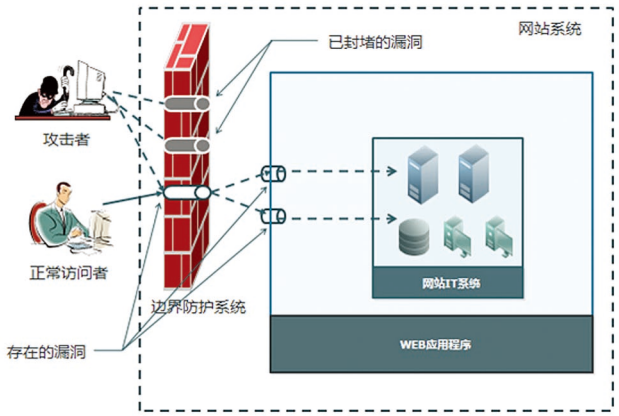


图 1.4　WEB 应用安全建设视图

3. 从生命周期构建安全的 WEB 应用

3.1 WEB 应用生命周期及对应的安全手段

现阶段，网站所面临的安全问题的有效防护和解决应贯穿于网站的整个生命周期，应在统一的监控、管理和指导下对系统、设备和人员有序的开展安全体系设计和建设。在 WEB 应用系统生命周

期里的每一个阶段都应该考虑如何通过技术手段落实安全需求，将安全手段融入到 WEB 建设的每一个阶段里。

一般来说，WEB 应用生命周期包括四个阶段，如下图所示：

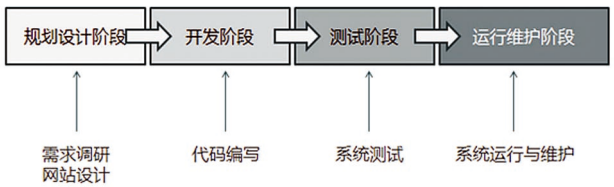


图 1.5WEB 应用生命周期

1) 规划设计阶段：规划设计阶段主要的工作是网站需求的调研和应用系统体系的设计。

在 WEB 应用规划阶段的主要工作，主要是制定相应的安全规划、安全目标及措施，同时需要对项目参与者，包括项目经理、开发人员以及质量管理人员进行安全意识的培训，提高对安全的理解和认识。

2) 开发阶段：开发阶段是开发人员实现需求的过程，主要工作为代码编写。

在 WEB 应用的开发阶段，特别是对于大型的 WEB 应用程序，如门户网站、网上营业厅等，参与开发的人员众多，安全意识、编码水平参差不齐，进行代码的安全审计就显得非常重要了。

3) 测试阶段: 测试阶段主要进行网站应用的测试，包括功能测试、性能测试、安全测试等。

在测试阶段里，QA 人员（非编程人员）不仅需要对门户网站进行功能测试，还需要进行完善的安全测试，如黑盒测试、渗透测试等。安全测试完成后，便可以交付给 WEB 系统所有者进入系统运营期。

4) 运行阶段：运行阶段主要的工作是系统上线及保障系统的正常运营，以及相应的维护。

在 WEB 应用生命周期中最主要的运营阶段，需要通过安全产品（如检测类、防护类、审计类等各类安全产品）和安全策略部署实现网站的稳定运营，其中最为重要的是周期性的进行渗透测试，风险评估等事前发现风险的工作，以指导安全建设。

3.2 通过绿盟远程安全评估系统构建安全的 WEB 应用系统

绿盟远程安全评估系统（简称 NSFOCUS RSAS）是绿盟科技研究团队多年研究成果的技术结晶，专门面向应用安全管理员进行应用系统上线前安全测试，上线后周期性安全评估的自动化风险管理工具。

其系统包含的 WEB 应用扫描模块采用了很多业内领先的技术，如模拟点击智能爬虫技术、主动挂马检测及核心调度引擎等，为用户提供最精准的检测结果及最高效的检测效率。相比传统 WEB 扫描器的仅局限于提供 WEB 应用层的漏洞扫描情况，该产品能够提供 WEB 应用、WEB 服务及支撑系统（网络层、操作系统层、数据库）等多层次全方位的安全漏洞扫描、审计、渗透测试和辅助逻辑分析，全面发现各类安全隐患，提出针对性的修复建议，以及形成多种符合法规、行业标准的报告。下图说明了 NSFOCUS RSAS 如何在 WEB 应用生命周期中协助不同职责的管理员进行 WEB 应用安全隐患的诊断。

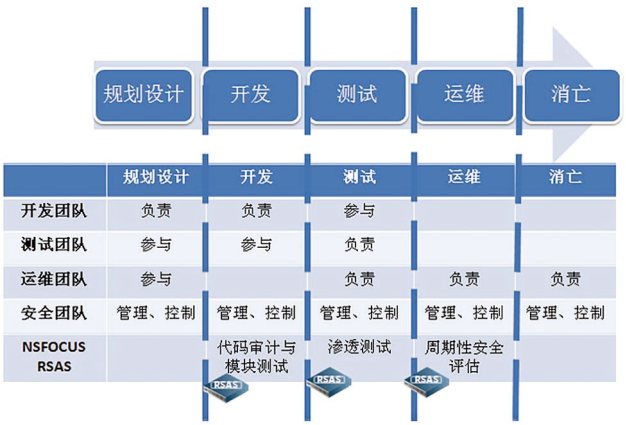


图 1.5NSFOCUS RSAS 在 WEB 应用生命周期中的应用

1) 规划阶段：

上文已经描述，在 WEB 应用的规划阶段安全方面的工作，主要是制定相应的安全规划、安全目标及措施，以及对人员安全意识和技能的培养。

这一阶段，可以采用绿盟科技的安全服务，对 WEB 应用安全设计部分进行规划、设计，并可以对项目参与人员进行安全技能培训。

2) 开发阶段：

在 WEB 应用的开发阶段，白盒与模块测试是非常重要而且必要的。白盒测试就是对程序的源代码进行检查，发现代码中的安全隐患。通过白盒测试和模块测试，将解决风险的过程前移，以非常低廉的成本发现程序中存在的重要漏洞。通过相应的源码安全审计服务，结合 NSFOCUS RSAS 产品，可以协助开发人员对编写的模块进行自我安全诊断，及早的发现安全隐患并修补。

3) 测试阶段：

在这一阶段，WEB 应用的安全性测试是一个非常重要的部分，传统上都是采用人工的渗透测试进行 WEB 应用的健壮性评估。人工的渗透测试一方面对测试人员的能力要求非常高，测试效果完全取决于该测试人员自身的技术水平；另一方面，测试周期长，人工测试效率低下，无法保证安全测试保质、如期完成。

在这一阶段，自动化的 WEB 漏洞扫描工具则可以发挥重要的作用。NSFOCUS RSAS 可以模拟黑客利用网页爬行(Crawling)技术，遍历应用中所有需要测试的链接，并对每个链接发送多种测试请求，诊断其有无漏洞可被利用，最后将结果呈现在用户面前。通过对目标站点进行自动化的全面渗透测试，可以大大提高工作效率，同时无需再依赖测试人员的个人能力，这样保证了整个渗透测试过程都在可以控制和调整的范围之内。

4) 运行维护阶段：

通过前几个阶段对 WEB 应用的安全检查、修补、加固等工作，开发者已经能够将一个相对安全、健壮的 WEB 应用正式推出给客户使用。运行维护阶段是在整个 WEB 应用生命周期中安全措施与管理最为重要的部分，除了必要的防护手段，该阶段一项最主要的工作是由安全管理员进行 WEB 应用的周期性安全评估，发现风险隐患及时修复。

通过采用 NSFOCUS RSAS，能够让管理员方便、有效地对

WEB 应用系统进行多层次、周期性的安全扫描，全面发现各类安全隐患，提出针对性的修复建议，以及形成多种符合法规、行业标准的报告，从而大大提高安全管理人员的工作效率。在操作使用方面，NSFOCUS RSAS 也独具特色，“一键式”操作模式设计，能够让用户通过最为简单的操作，获得专业、全面的评估报告。另外，多用户、多权限划分的用户管理方式，能够由一台设备虚拟成面向多用户独立使用的虚拟设备，从而为用户带来最高性价比产品，节省用户投资和管理开销。

相比普通 WEB 应用扫描器，NSFOCUS RSAS 采用专用硬件平台和嵌入式操作系统，以及优化的核心调度引擎，能够提供业内最为高效的检测效率。同时结合多级分布式部署，可以对多个网站群同时并发进行漏洞扫描和风险评估工作，所有扫描结果数据可以由管理节点进行统一的数据汇总、分析和报表呈现。

绿盟远程安全评估系统将传统系统层、网络层与应用层漏洞检测相结合，改变了传统系统扫描器仅局限于系统层和网络层的相关漏洞扫描，而 WEB 扫描器仅局限于提供 WEB 应用层漏洞扫描的局面。同时，该产品紧密围绕“漏洞管理”的工作流程，通过划分漏洞预警、漏洞检测、风险管理、漏洞修复、漏洞审计等五个周期性阶段，在国内首创了“开放漏洞管理”工作流程平台。基于这个开放平台，绿盟远程安全评估系统将“漏洞管理”理念贯穿于整个产品实现过程中；此外，该产品还可以通过多种二次开发接口与其他安全产品协作来完全实现风险管控的整个工作过程，帮助用户打造完善、智能、全生命周期的风险管理的体系。

图 1.5 NSFOCUS RSAS 开放漏洞管理过程图

4. 小结

通过上述对 WEB 应用现状和常见的威胁的分析，我们可以看出，目前因特网上的 WEB 应用，存在着极大的安全隐患和风险，政企单位对 WEB 应用安全的保护及漏洞风险的管理，已经刻不容缓。

绿盟科技全新的 NSFOCUS RSAS 产品，综合应用了很多业内领先的技术，为用户提供精准的检测结果及最高效的检测效率。可以用于网站管理员进行 WEB 上线前安全测试，上线后周期性安全评估以及企业安全管理员进行统一的风险监控与管理，形成一套端到端的完整 WEB 应用安全解决方案，为企业的 WEB 应用保驾护航。

历经多年的不间断技术创新和产品研发，绿盟远程安全评估系统已经成为这一领域的领导品牌，得到运营商、金融行业、互联网公司、政企以及风险测评机构等用户的广泛认可，绿盟科技也成为国内惟一一家能够面向全行业用户提供多层次漏洞管理解决方案的专业厂商。

参考文献：

【1】吴海燕，苗春雨，刘启新，孙方成 . WEB 应用系统安全研究综述 [R]. 北京 . 清华大学计算机与信息管理中心，2007:2-4.

【2】李钠 . WEB 架构及安全防护剖析 . 北京 . 绿盟科技 .2009:07

【3】田民 . 运营商门户网站安全建设思路 . 北京 . 绿盟科技 .2009:07

【4】oel Scambray, Mike Shema,Caleb Sima. Hacking ExposedTM WEB Applications. 2008

【5】ZDnet. 2008.《SQL 注入攻击第三波浪潮袭来》. http://security.zdnet.com.cn/. [联机] 2008 年 7 月 . http://security.zdnet.com.cn/security_zone/2008/0708/968547.shtml.

【6】Gartner. 2009.《Gartner Says 20 Percent of Commercial E-Mail Market Will Be Using a SaaS Platform By the End of 2012》. http://www.gartner.com/. [联机] Gartner, Inc., 2009 年 4 月 .http://www.gartner.com/it/page.jsp?id=931215

【7】OWASP. http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

电子政务外网介绍及安全建设思考

行业营销中心 孙铁

摘要：国家电子政务外网是我国电子政务的重要基础设施，也是《国家信息化领导小组关于我国电子政务建设的指导意见》（中办发[2002]17号）和《国家信息化领导小组关于推进国家电子政务网络建设的意见》（中办发[2006]18号）文件确定的重点建设任务。如何建立电子政务外网信息安全保障体系，为政务外网上运行的政务业务及服务顺利运行提供保证，是全网建设的重点。

本文在对电子政务外网及其安全建设简单介绍的基础上，初步描述了电子政务外网安全建设思路，为以后进行更为详尽的方案设计打下良好基础。

关键词：电子政务外网 17号文 18号文 988号文

1 电子政务外网简介

国家电子政务外网是我国电子政务的重要基础设施，也是《国家信息化领导小组关于我国电子政务建设的指导意见》（中办发[2002]17号）和《国家信息化领导小组关于推进国家电子政务网络建设的意见》（中办发[2006]18号）文件确定的重点建设任务。

电子政务外网是服务于党委、人大、政府、政协、法院和检察院的政务公用网络，覆盖中央、省、地、县四级政务部门，主要满足各级政务部门社会管理、公共服务等面向社会服务的需要，支持电子政务业务系统和国家战略性、基础性信息资源库的运行，支持跨部门、跨地区的信息资源共享和交换。

作为我国电子政务总体框架的重要组成部分和电子政务的重要基础设施，国家电子政务外网就是要依托传输骨干网构建的IP网络，为各级政府部门提供专用网络服务，解决电子政务建设中重复建设、资源利用率低、信息共享和业务协同难等问题。建设一个公共的政务网络有利于各级政务部门开展社会管理和公共服务，有助于加快服务型政府的建设。

根据中办发[2002]17号文件和[2006]18号文件提出的“建设和整合统一的电子政务网络”，促进信息共享、业务协同的总体要求，国家电子政务外网自2005年起正式启动建设，经过几年的努力，目前一期工程已经完成，初步具备了承载部门业务应用的能力，一些部门和地方的业务应用已在政务外网上运行。

1.1 服务对象

电子政务外网的服务对象是党委、人大、政府、政协、法院、检察院的各级政务部门。

1.2 承载业务

非涉密业务应用，各级政务部门管理和公共服务的业务。

1.3 覆盖范围

由中央政务外网和地方政务外网组成，横向连接党委、人大、政府、政协、法院、检察院的各级政务部门，纵向覆盖中央、省、地市、县。即通常所说的横向到边，纵向到底。

1.4 建设情况

政务外网建设目标是：依托统一的国家电子政务通信传输网络，整合建设电子政务外网，支持电子政务业务系统的运行，支持跨部门、跨地区的信息资源共享，支持电子政务业务的互联互通和信息交换，促进政府监管能力和服务水平的提高。2010年底前要基本建成横向到边、纵向到底的纵向四级

网络，以满足国家电子政务发展的需要。

目前中央政务外网一期工程已基本完成，具备了为中央和地方政务部门提供网络支持服务的能力。横向已经连通在京的 48 个中央政务部门，纵向实现了与 32 个省级节点单位的对接，建设了外网网管中心和外网网站，初步形成外网服务体系；初步构建外网信息资源目录体系与交换体系，建设外网数据交换中心原型；目前，国务院应急办、中纪委监察部、国家审计署、国家安监总局、文化部等 8 个部门已经依托国家政务外网开展 12 项业务应用。国管局、新华社、空间地理库等单位或项目也计划利用国家政务外网开展相关的跨部门、跨地区的业务应用。

省级电子政务外网建设从总体上看，各地发展还不平衡。有的地方政务外网建设较早，北京、江西、浙江、广东等已覆盖到县，并已经开始承载中央和地方的业务应用；也有的地方如西藏、陕西省级政务外网平台尚未建成，目前可以通过临时过渡网络来满足一些中央部门在地方的业务需求。

1.5 下一步工作重点

为了进一步推动和规范政务外网建设，尽快形成政务外网整体服务能力，下一步将在国家主管部门的支持下，重点推进下列工作：（一）加强协调，理顺管理体制；（二）加快网络建设，拓展网络覆盖面；（三）完善服务体系，提高服务水平;（四）明确责任，保障网络和信息安全。

2 文件依据

电子政务外网的建设主要依据以下三个文件：

2.1 《国家信息化领导小组关于我国电子政务建设的指导意见》（中办发 [2002]17 号）

17 号文要求：“十五”期间，我国电子政务建设的主要任务之一就是建设和整合统一的电子政务网络。为适应业务发展和安全保密的要求，有效遏制重复建设，要加快建设和整合统一的网络平台。

17 号文规定：电子政务网络由政务内网和政务外网构成，两网之间物理隔离，政务外网与互联网之间逻辑隔离。

政务内网的主题包括党委、人大、政府、政协、法院和检查院等六大系统业务网络及其顶层互联的网络，该网络将以传输和承载涉密业务和敏感度高的内部信息为主。

政务外网是政府的业务专网，主要运行政务部门面向社会的专业性服务业务和不需在内网上运行的业务。

2.2 《国家信息化领导小组关于推进国家电子政务网络建设的意见》（中办发 [2006]18 号）

18 号文进一步明确了国家电子政务网络建设的基本原则：需求主导，统筹规划、整合资源、服务应用、着眼发展、注重安全。

规定了国家电子政务网络建设目标：用 3 年左右的时间，形成中央到地方的国家电子政务传输骨干网，建成基本满足各级政务部门业务应用需要的政务内网和政务外网，健全国家电子政务网络安全保障体制，完善国家电子政务网络管理体制，为电子政务发展提供网络支持。

2.3 《关于加快推进国家电子政务外网建设工作的通知》（发改高技 [2009]988 号）

为了加快国家电子政务外网建设，推进部门应用在政务外网上的部署，充分发挥国家电子政务公共设施的作用和效能，国家发改委和财政部联合印发了《关于加快推进国家电子政务外网建设工作的通知》（发改高技 [2009]988

号）（以下简称 “988 号文”），进一步明确了国家政务外网的建设目标和任务，并就推动政务外网的工程建设、业务应用、安全保障和运维服务等提出了相关要求。通知要求：

国家政务外网的建设目标是：力争到 2010 年底前，基本建成从中央到地方统一的国家政务外网，横向要连接各级党委、人大、政府、政协、法院、检察院等各级政务部门，纵向要覆盖中央、省、地（市）、县，满足各级政务部门社会管理和公共服务的需要。

尚未实现与国家政务外网连接的部门，要按照统一的标准和规范，于 2010 年初完成接入国家政务外网的工作，要尽快将各类可在国家政务外网上运行的业务系统向国家政务外网上迁移，各级政务部门要根据国家关于等级保护的有关规定进行安全建设。

要加强国家政务外网的信息安全保障工作。中央和地方政务外网的建设和运维单位，要切实落实网络安全保障责任制，明确国家政务外网信息安全主管领导和工作部门，建立健全安全管理制度。要按照国家政务外网统一规划，建立网络安全防护体系和统一的网络信任体系。要定期对中央和地方政务外网进行安全检查，对查出的安全隐患和问题及时进行整改，确保国家政务外网的安全可靠。

各级政务部门要根据国家关于信息安全等级保护的有关规定，确定国家政务外网上运行的业务系统的信息安全等级，采取相应的信息安全等级保护措施，进行信息安全风险评估，保障各自业务系统的信息安全。

为避免重复投资、重复建设，充分利用好国家已建电子政务公共设施，国家发改委今后不再批准建设新的部门专用业务网络。财政部门原则上不再安排新的部门专用业务网络运行维护经费，并将根据各政务部门业务系统在国家政务外网上部署的进展情况，相应调整业务系统的运行维护费用，同时合理安排国家政务外网运行维护费用。

在 “988 号文” 中有几个要点：1、2010 年前将实现政府各类业务应用向政务外网的迁移工作，完成目标是纵向到底，横向到边；2、迁移的业务系统将按等级保护的相关要求进行建设；3、财政和发改委原则上对新建的部门专网不予审批，对已有的不予运维支持。

3 电子政务外网安全建设情况

目前国家层面电子政务外网安全保障体系一期建设已经基本完成，正在规划安全二期的建设，一期主要目标是：建成政务外网网络安全防护体系、网络信任体系、安全管理体系和统一的技术标准规范体系，保障电子政务外网的安全可靠运行与有效的应用。

● 安全防护体系

针对国家电子政务的安全需求和面临的安全威胁，在防护体系上采用了如下防护技术和手段：

- 防火墙系统
- 网络入侵检测系统
- 抗拒绝服务系统
- 防病毒网关
- VPN 网关
- 安全认证网关
- 网管中心主机加固

● 网络信任体系

已建立了 CA 中心，具备证书发放能力。监察部的纠风业务系统作为政务外网信任体系的第一个应用，已经与 CA 系统成功对接。目前正在使用和决定使用外网数字证书的单位有中纪委监察部、国家发改委、扶贫办、审计署、国土资源部、新华社、国务院应急

办、北斗导航卫星等。

● 安全管理中心

初步建立了一套较完善的网络管理及监控系统，完成安全预警管理、安全监控管理、安全防护与响应管理、安全追踪管理等功能。

● 安全管理体系

制定并不断完善各项运维规章制度。

以上是国家层面电子政务外网安全建设情况，各省市的电子政务外网安全建设发展还不平衡，总体来看覆盖面也不够，特别是各地方外网安全建设仍处于没有统一指导、各自为战的状态，这样给电子政务外网安全的统一部署和集中管理带来了很大困难。

4 电子政务外网安全建设思路

“988 号文件”要求在 2010 年底前，基本建成从中央到地方统一的国家政务外网，在政务外网四级网络的建设和运行过程中，系统安全保障体系建设是一项重点工作，依据实际应用情况，充分平衡好安全投资与安全需求之间的关系，根据预警和风险评估结果，不断提升安全防护的适应性。在全国电子政务外网安全建设中应关注如下重点工作：

4.1 安全基线

目前电子政务外网整体安全建设不统一、各自为战的状况，直接影响了电子政务外网整体安全思路的贯彻和安全策略的统一部署、影响了中央政务部门的业务开展，影响了国家政务外网整体效益的发挥，影响了中办发 [2006]18 号文件提出的用 3 年左右时间，建成政务外网目标的实现。

因此，安全基线建设是政务外网安全建设的基础，安全基线是以现有比较成熟的安全技术为基础，围绕承载业务及数据的安全需求，划分业务类，构建业务安全池，对安全池进行封装，在安全池中借鉴面向对象的设计方法和工具，设计满足业务系统安全需求的基线安全体系。

安全基线包括以下两个方面：

● 政务外网自身安全基线

由于电子政务外网分为四个层面（国家、省、市、县），因此应设定四个层面的安全建设基线，对于国家、省外网的基线应着眼全面、合规，应具备检查、监管和态势感知的能力，而对于市、县级电子政务外网应以安全技术手段的实施达到防护目的作为重点，这两级网络应作为政务外网的神经末梢，除了具备必要的防护能力外，还应将收集到的安全状况数据上传到上级分析节点。

● 连接到政务外网各单位业务系统的安全基线

对于连接到政务外网的业务系统应按照其业务安全需求规定相应的安全基线，对入网系统按安全基线要求通过技术手段和管理手段进行检查，以保证业务的正常开展以及电子政务外网基础服务不受影响。

在各地政务外网建设运维单位的行政隶属关系、安全建设水平不尽相同的情况下，如果要切实发挥中央网管中心的作用，解决在运维服务过程中“工作协调难，体制不顺”的问题，安全基线建设是一个非常好的解决办法：制定统一的技术规范、服务标准、协同工作流程和运维服务考核办法，并通过技术手段进行检查；地方政务外网的建设运维单位按照统一的标准规范和相关要求进行建设和运维，同时在做好本级政务外网建设安全运维工作的同时，制定对下级建设运维单位的安全基线规范，建立本地的协同工作机制，最终形成全网上下协同一致，反应快捷的运维服务体系，确保国家政务外网的稳定运行，为建立全网

高效快捷的运维服务体系奠定基础。

4.2 分层次进行安全设计

电子政务外网的安全建设不能采用一刀切的方式进行建设，这样也违背了政务减少重复建设、节约投资的原则。

因此，应对四级外网进行区分，对国家、省、市、县的电子政务外网进行分层次的安全体系设计，同时也应根据各地信息化发展水平和电子政务外网隶属关系的不同进行适合本地特点的安全体系设计。

但设计的原则应保证与上级网络实现互联互通、资源共享、业务协同的实现。

4.3 等级保护

应在进行电子政务外网安全设计中遵循国家等级保护政策，保障网络基础安全。电子政务外网对于网络的安全保护按照如下等级要求进行：中央网络管理中心局域网、中央城域网接入单位的网络管理中心局域网和各省市节点的二级网络管理中心局域网，至少达到第三级；中央城域网接入节点单位和各省市的网络，至少达到第二级。

4.4 安全监控

应建立政务外网全网及省级监控平台，捕捉并及时处理安全事件，保障网络稳定运行，同时对全网信息安全态势具有分析功能。

监控平台实现的功能包括：

网络流量的实时监控和异常流量检测

入侵行为检测

访问行为的审计和还原

非法访问诱骗及监控

网络攻击预警

攻击场景的还原、呈现、取证

未知恶意代码和攻击手段的发现

态势感知和分析

4.5 网络信任体系

按照中办发【2003】27号文的要求，国家政务外网网络信任体系的建设是电子政务外网建设的重要内容之一，“988号文”也要求建设统一的网络信任体系。目前国家电子政务外网和一些省的电子政务外网已经建立了电子认证服务体系，

应建立由“政务数字证书系统”及其省级RA、部委RA等相关服务设施与服务人员组成的服务和技术支撑体系，承担为电子政务外网用户发放、管理数字证书以及提供其他相关服务。

4.6 安全应急

建立应急响应组织、技术、管理体系，制定相应的信息安全通报制度和应急预案并建立演练制度，提高对突发事件的反应能力。

5 总结

总之，从全局视角思考和建设政务外网安全保障体系，最大化提供网络的可用性，建立一个畅通、安全和可靠运行的国家政务外网，充分保护、利用和延伸原有安全体系资源，建立能够支撑网络运营的全局管理、防护监控、预警、响应和服务等辅助保障的技术、管理体系是政务外网安全保障体系的目的。

通过保障体系的建立和实施，形成全网三大能力，即：

- 及时发现和定位的能力
- 有效防护和处置的能力
- 快速响应和恢复的能力

参考资料

[1] 加快推进国家电子政务外网建设的八方面意见

[2] 国家政务外网电子认证服务体系建设

[3] 国家政务外网信息安全管理和保障的思路

基线式安全与蝴蝶效应

—论电力信息安全的持续测量、多维保障与运维绩效

行业营销中心 张书嘉

摘要：文章旨在依据电力单位与行业所需—规避那些制约着生产输配进程、对公服务信誉、以及 IT 应用资产的稳健运行的问题；推理一种适度保障和提升运维周期绩效的解决思路。

关键词：电力 基线式安全 持续测量 多维保障

SUMMARY

本文藉于理解“智能电网的发展趋势与保障目标、调度自动化的防护控制与远程集约监管、等级保护的合规要求与行业化适用、IT 对公业务节点的威胁隐患”等关键因素，进而剖析电力系统可能隐而未现和随机扩展的安全隐患与运维短板，引申说明“基线式的安全测量与配平理论、工具”的行业适用性—它将满足电力系统的本地化安全内控目标、应对全部的合规性约束、提升监管水平与运维绩效、完善持续改进能力的期望。

开篇以前，澄清三点科普性问题将有益于引申本文的关键要点和创意。

“蝴蝶效应与安全实效保障的辩证观点”：

1、何谓信息安全的蝴蝶效应?

Ans.:因事物周期中的量变而引起的质变[唯物辩证法]；当电力系统被赋予一组业务使命和运行目标时，其个体／群体的事前安全基础条件的理想程度，将决定其业务使命是否能够稳健和持续运行，以及电力系统在服务过程中是否可避免潜在的短板和损失；这种普遍的非线性关系即是蝴蝶效应。例如：忽略了系统实用化运行之前的初始安全评价和补偿，或许导致其隐含的漏洞被连锁式的利用；进而成为入侵者所期盼的美丽的误会。结论：初始的安全条件决定业务信誉与风险控制能力，当面向一组电力系统，如加以及时的事前安全测量和调节，以及事中的适度监控和配平，即可确保未来运行／运维过程中减少顾虑，进而提升绩效。

2、如何事前认知蝴蝶效应及其隐含的安全隐患?

Ans.:蝴蝶效应是潜在安全隐患的引喻。信息系统自身安全性及其所承载的业务使命的保障要求均应当被测量，意在获知“其理应具备的理想安全水平”，以此安全水平作为衡量基线，持续的监控、维护和调节这一安全基线，以确保信息系统在任意时间条件和环境条件下均可被调节为理想的运行状况，保障业务资产的稳健和服务信誉；上述的处理过程并不在于提高系统的强壮性，而意在消除事前隐患，优化事中防护措施的针对性，优化运维过程的实效性。

3、为什么需要借助测量手段发现和监管蝴蝶效应之隐患?

Ans.:安全基线的定义是意在确认最佳保障目标和当前差距，进而实现针对性配平，而动态的测量／考核安全基线的执行程度，将有助于形成持续改进的安全监管闭环；其中测量方法的运用将更具体的实现下述意义：

- 事前了解到可能疏于防范的环节；
- 了解保护到何种程度为最理想安全水平；

了解系统当前运行状态与之的差距；确保更加理想而适度的安全基建与技改投入；

■ 通过测量，为每类系统、每个阶段分别制订理想的安全水平，形成持续改进机制；

■ 实现本地符合性管理；确保针对各类政策／标准的行业化、本地化适用；

■ 将安全保障和运维任务，与业务稳定运行的评价考核指标结合在一起；形成集约性的安全评价与督导能力，同时以此优化运维绩效，强化向下垂直管理的机制。

本文的最终论点与创意即意在解答如下的疑问：

■ 如何识别面向各级各类信息系统建立差异化的安全测量、配平?

■ 如何依据电力实际情况，领会基线安全的全过程，并实际运用于各类电力单位?

■ 如何提升专责式的运维绩效，并实现科信单位的向下集约考核与集约监管?

■ 如何在安全工程建设中形成理想的基建和技改效果，并由此获得创新成果?

SOLUTION: 基线式的测量、控制、决策支持

上述第“3”个观点提示了电力单位的实际需求，它概括了电力系统对于本地化的安全内控、提升监管水平与运维绩效、应对合规性约束、完善反应效率与持续改进能力的期望。

本小节意在陈述实现上述目标的机制，以及“基线式安全模式”的包含组件、执行方法与运维过程，即意在解答如下的疑问：

制订安全基线、执行安全基线的方法与过程为何?

安全基线的集约监管，以及形成持续改进机制的过程怎样?

面向一个真实的电力单位，基线式安全模式如何落地?

1.1 意义与定位

“基线式安全”应用于电力系统的核心意义、及功能定位?

Ans.: 基线式安全在于事前测量短板、事中集约监管、事后调理改进；相对于传统安全机制可能隐含的“事前的疏忽→事中的短板→事后的风险损失”的连锁效应；“基线式安全”则通过测量与配平的手段强化防护水平，并基于此提升合规性管理、评价考核和持续改进能力。

其意义在于：

■ 避免过度保护：综合测量全局信息系统，分析理化的安全水平，分项补偿／配平；

■ 确保补偿／配平后的安全水平与理想水平相吻合，并持续考核和监管该水平；

■ 可适时针对当前基线水平进行微调：微调的条件包括：发现了最新的威胁／漏洞、敏感时期的特殊政策或保护要求、新系统的实用化运行、组织变动或业务变动。藉此形成持续改进的 PDCA 闭环。

Postscript: “基线式安全”是适用于电力单位的解决方案；它由一套分析模板、一组中立性的工具集、一个轻量级的监管平台实现。基线的测量与制订将协助安全专责及时发现那些疏于防范的环节，制订理想化的安全水平，并加以适度的配平和监控；优化电力单位的业务保障能力、运维绩效与科信部门职能。

1.2 过程与实现

■ 基线安全的初始过程：定义目标、制订基线、差距分析、评测基线、适度配平；

■ 基线安全的运维过程：监控基线、集约

考核、决策支持、适时微调、维护闭环；

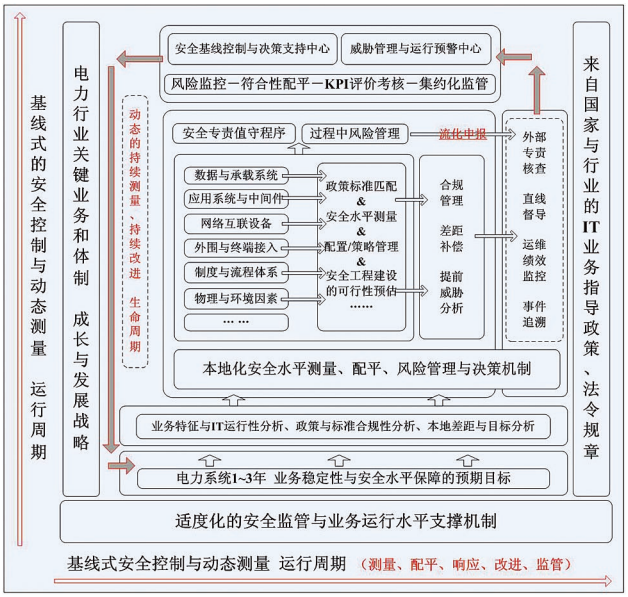
上述过程支撑着基线式安全模式的工程目标与应用收益，并包含基线式工具平台的搭建与运维机制；如下的三段陈述则是对“基线”的工程化说明：

■ 第一阶段，定义目标与制订基线：测量电力单位所需的理想化安全建设目标与当前水平的差距，同时结合本地保障要求、业务特点和政策法规指引等因素，制订适用于本地的合理安全基线；它将确认安全建设程度、投资重点和持续保障水平；

■ 第二阶段，试行与配平基线：新的安全水平（基线）是面向各级各类信息系统分别定制的“差异性和互补性的安全策略”，作为“维持电力系统稳健运行的一组最佳指标”，基线必须完全契合于各信息系统的保障要求，经过试行和评测后的基线将被落实应用，各类系统依据各自的基线指标被适度巩固的过程称之为“配平”，这一过程确保它们均达到“理想的安全水平”；

■ 第三阶段，监控与维护基线：确保各类信息系统在运行周期中被针对性保护和持续保护，监控基线的应用情况将确保各系统“仍然保持于一个理想的安全运行水平”；然而，当出现最新的威胁／漏洞、敏感时期的特殊政策或保护要求、新系统的实用化运行或业务变动等情况时，可适时针对当前基线水平进行考核与微调。藉此形成持续改进的 PDCA 闭环；这一创意兼隐含了集约化监管、运维绩效评价考核的意义。

如下带有复古风格的示图意在澄清“基线式安全模式与实用工具”的运行机理：



示图—电力系统之“基线式测量与风险管理机制（闭环）”

事实上，更多的安全焦点关注在疏于内控，而非系统漏洞或外部攻击；相对传统安全保障模式的臃肿而繁重，基线模式更加适度和可控。基线是“维持电力系统稳定运行的一组最佳指标”，即是“一个 IT 业务节点上线时理应具备的安全水平”。制订和补偿这一水平可能带来新的采购，然而多数时候只是调节安全配置和策略、优化制度体系即可。

上述的“基线安全模式示图”同时隐含了如下几个值得思考的安全保障焦点：

■ 安全防护与内控运维需形成差异化，以确保分项补偿、合理配置；

■ 安全保障需有所依据，它们包括：本地的预期保障目标、政策 / 标准、业务特点等；

■ 安全运维应与指标体系和集约化管理模式相结合，确保联合响应和直线督导；

■ 安全建设应当适度投入，且需事先进行可行性评价；

“基线式风险管理设想的实施过程”机制可以适时地识别 IT 资产的安全性浮动情况，从而自主生成“符合基线标准（理想水平）的补偿方案、配置指令、策略改进和决策支持建议”。基线模式为各类系统构建一种自我测量与考核能力，协助那些未符合“理想安全水平”的 IT 节点或制度条款进行配平，并依据特定所需进行微调和改进，在信息资产的运行周期中形成保持于理想安全水平的保障闭环；保障闭环能够面向各类信息系统和制度体系给予综合性的监管；并适时测量和验证当前安全策略的有效性。

然而所见上述机制，IT 业务资产的生存性亦可从事前、事中和事后三个阶段给予维护，确保安全事件在触发之初被测量和控制，在入侵者行使其意图的过程中被阻断和补偿，确保当资产遭遇威胁时，风险能够被追溯，安全策略能够及时响应和及时微调。

基线安全模式能够将上述机制／机理适度的贯穿于信息资产的运行周期中；使各阶段、各层面的安全机制相互补足而形成体系，避免了安全保障的重复实施和过度投资。

如下的表格陈述了基线安全模式在新建、防护与运维过程中的意义和职责：

基线安全的初始过程：
定义目标：面向各级各类信息系统，定义一个结合业务特点、政策要求和实际应用的保障目标；
制订基线：面向各级各类信息系统的保障目标，量化定义一组“适用性策略、配置或补偿标准”；
差距分析：结合基线（理想安全水平）的指标要求，评价当前信息系统与之的差距；
评测基线：确认“基线“的指标集合以及策略集合的可行性；
适度配平；针对当前信息系统与理想水平的差距，依据“基线指标和策略集合”为之补偿；
基线安全的运维过程：
监控基线：在 IT 运维过程中，持续监控各 IT 资产的安全性浮动情况，即与基线水平的差异；
集约考核：面向 IT 绩效相关单位，评价其资产运行健康性、政策合规性和安全投资可行性等；
决策支持：依据安全投资与安全水平运维的考核结论，确定向下督导、监管或约束的操作模式；
适时微调：面临新的风险、新的合规性约束、新系统实用化上线或业务变动时，适时微调基线；
维护闭环：对于“一个理想安全水平”进行周期性的有效性评价和改进，确保持续的合理化。

1.3 应用的场景

本小节旨在依据上述的安全保障模式，如下模拟了一个真实应用场景—即 ABC Grid 的应用场景；以期求证“基线安全模式”于电力行业的适用性：

A、背景：

■ ABC Grid 是由总部直接管辖和督导的地区型电力公司，承担地区电力输送、供配、营销职能；

■ 下属 15 个供电单位，部分单位新近成立；信息化水平参差不齐、新旧不一；

■ 预期任务 :2010 年须启动完备的安全建设，以期提升本地的内控与对公业务的运行稳定性，提升专责模式的运维绩效、提升科信部门的集约管理能力；并期望符合等级保护、春秋检、敏感时期政策要求等规则规范。

B、面临的传统安全建设问题：

■ 安全建设过程中，新的安全投资不易避免过度投入；

■ 不易估测安全建设／采购的可行性，以及验证其建设效果；

■ 对于新式威胁和新近政策要求的应接不暇；

■ 更多的安全设施，更多策略配置与应用；安全专责体制的运维压力加大，绩效降低；

■ 除了日志管理，几乎没有更实效的手段进行垂直监管和督导。

C、基线式安全的实践过程：

■ 过程一：依据本地的业务特点和安全需求，制订保障目标、制订全局 IT 系统的安全基准线、优化制度 / 流程体系、制订用于集约监管和优化运维绩效的 KPI 考核集、制订特定政策 / 标准的本地化适用方案；

■ 过程二：确认上述理想化的指标（安全基线）的可行性，进行差距分析；

■ 过程三：依据差距分析结果，针对性的规划设施利旧、新建与策略调整、优化制度与流程体系；

■ 过程四：将上述过程中形成的基线指标和策略导入“基线核查工具与决策支持平台”，监控各级单位、各类信息系统与基线安全水平的符合情况，对违规情况进行配平和直线督导，（此过程可与现行的操作票和专责制度结合在一起）。

D、过程中的交付成果：

1. 各级单位、全局信息系统的安全基线标准（理想安全水平及其补偿策略）；

2. 安全差距—目标分析报告；

3. 特定政策、标准与法规的符合性声明，以及本地化遵从方案；

4. 最近一次安全建设的解决方案（利旧、新近采购、策略／配置调整规划）；

5. 业务持续性与安全运维的 KPI 评价考核标准和指标库；

6. 基线持续改进标准与实施方法；

7. 用于测量和配平的基线核查工具集、用于评价和监管的决策支持平台及其电子化模块／接口。

E、应用效果与新的运维场景：

1. 科信部门观察各级单位／系统的安全基线运行情况、直线督导和评价下游单位的基线配平；

2. 当面临特定政策／标准的测评时，形成针对此政策标准的符合性声明，以证明本单位的合规性；

3. 当本单位或下游单位开始新的安全建设或采购（基建／技改）之前，可依据基线指标，评估本次安全投资的可行性与必要性，确认是否通过采购的方式补偿差距，或仅通过调整策略配置即可；

4. 针对 IT 业务节点的运维绩效进行评价考核，提升信息系统的防护水平和生存性；并适时监控和微调基线，以确保基线水平的有效性，形成持续改进机制。

TOOLKIT: 基线控制、决策支持与预警中心

如前图示，各种测量和分析结果以及运维过程中的指标数据均被上溯至“两中心”，由两中心实现统一的基线配平与评价考核，符合性管理和风险控制机制等；进而对于违规情况或薄弱环节进行定位，将控制指令或预警信息下溯至相关的安全设施，或通报给安全专责；以督导违规单位或系统依据基线安全水平进行补偿和配平。亦可依据当前的时势或政策标准要求，对基线水平进行微调和持续完善，由此修正后的结果再次上溯至“两中心”，以验证新的基线水平的可行性，周期性循环往复，形成基于测量→配平→评估→改进的 PDCA 闭环。

“两中心”的职能特点与工作模式，如下：

■ 安全基线控制与决策支持中心：差距分析的结果以及安全基线标准通过工具化手段写入该中心的知识库，由该中心负责维护各阶段的安全水平，例如奥运期间的安全水平、六十年国庆期间的安全水平、日常安全水平等等。该中心依据基线标准针对各级各类别信息系统进行适时的核查，审核特定系统的安全防护指标与合规性情况，对于存在“安全差距”或未符合基线标准的系统进行预警并出示整改／补偿建议。

P.S: 该中心可依据各类安全保障要求、业务特点和政策法规来定义新的安全基线标准，确保安全水平的持续可控、迅速反应；

■ 威胁管理与运行预警中心：当电力单位具备私有的安全基线标准和执行能力时，惟一的保障缺陷仅在于“对于外来未知风险的防护不敏感性”，即现有的基线安全体系能够确保各类信息系统随时符合理想的安全水平、符合政策标准、符合业务特点的所需等；但对于未知 / 新发现威胁的防卫反应性不足，因而该中心用于弥补这一点，能够适时采集世界范围内的最新漏洞信息并评价本地系统是否存在被攻击的可能，或适时采集特定地区暴发的病毒或木马信息，进而提出及时的预警和补偿方案。

■ 集约化管理能力：“两中心”同时旨在优化上游单位的垂直监管职能，例如：

可适时监控各所属下级单位的关键业务运行情况、安全水平符合情况、合规情况等；

对于违规情况适时的提供整改方案，监控整改效果，以及更新 KPI 指标的评价分值；

能够对于下属单位的安全建设／投资项目申报进行审核，进而确定是否需要追加新的安全投资以补足安全差距和提升防护能力；并对

采购名录和安全建设方案进行合理指导。

总结：“垂直监管→集中核查→流化申报→精确测评→直线督导→持续改进”机制完善了上游单位的安全监管职能。

BENEFIT: 电力单位－基线安全实践的适用性与收益

本小节论证 ABC Grid 构建基线式安全的应用效果，藉此确认“基线式安全”对于电力单位的适用性与收益。

基线式安全的应用收益：

- 测量和补足安全差距—中立性技术、完备性规划；谋全局而不偏重一技；
- 符合性管理—国家／行业标准的本地化、实用化；
- 策略与配置的统一调度—实现各级／各类信息系统的安全策略与配置的统一管理和调度；
- 集约管理与运维 KPI 的实效性—优化科信／调度自动化部门的垂直职能和运维绩效；
- 评估安全工程 / 采购的可行性—适度保护、合理投资、建设效果可验证；
- 提升集约化能力—垂直监管→集中核查→流化申报→精确测评→直线督导→持续改进。

基线式安全的应用可行性：

- “基线式安全”采用轻量级方式实现，应用中立技术，电力科信部门可自主掌握；
- 可完全契合现行的电力业务特点、制度体系、专责管理机制，科信部门职能等因素；
- “基线式安全”是契合于本地实际情况的标准化产物，可持续履行，持续改进；
- 经济效益：“基线式安全”旨在维护适度安全建设，因其是基于业务的测量、基于差距的补偿；可避免重复投入、重复建设；
- 行业效益；“基线式安全”可促使 SG186 安全保障体系与评价考核体系完美融合；可作用在智能电网的安全集控与合规；可面向调度中心、集控中心、厂站提供安全水平的集约监管；
- 创新价值：“基线式安全”使所有信息系统的安全水平、运维绩效都成为可测量的、可考核的、可改进的；其质变的思想可应用于科信单位、调度单位或智能电网中，均可形成创新性成果。

POSTSCRIPT

“基线式安全”的功能定位：适度化保护工具、符合性管理工具、集约化监管与评价考核工具；

“基线式安全”的适用范围：电网／发电企业的区域单位、二级调度单位，电网／发电企业的总部或第三方监管机构；

“基线式安全”的真实案例：绿盟已协助中国移动集团构建了全体系的安全核查、评价考核、合规性管理与集约监管能力；

“基线式安全”是新的 IT 业务保障与运维模式：相对于传统式安全建设的臃肿而繁重；基线式安全更加适度而可控。本文依据电力单位与行业所需，从蝴蝶效应的测量与内控角度推理了一种适度保障和提升运维周期绩效的解决思路。进而能够密切契合电力单位的业务保障目标，提供理想的安全解决方案和行业化产品；协助电网单位保持自身的理想安全水平，优化安全建设的投资成效。

WAF vs IPS 谁更适合防护WEB应用？

产品市场部 秦波

摘要：IPS（入侵防护系统）和 WAF（WEB 应用防护系统）两款产品有不同的使用场景，随着 WEB 应用复杂度的提升，对安全性的要求也日趋增高，WAF 产品应运而生。本文从对比角度来分析，是为了从差异中让读者更清晰地理解 WEB 安全防护产品的技术特征。

关键词：WAF IPS WEB 应用防护 绿盟科技

谁是最佳选择？

WEB 应用防护无疑是一个热门话题。由于技术的不断成熟和人们对便利性的期望越来越高，WEB 应用成为主流的业务系统载体。在 WEB 上“安家”的关键业务系统中蕴藏的数据价值引起攻击者的青睐，网上流传的 WEB 漏洞挖掘和攻击工具让攻击的门槛降低，也使得很多攻击带有盲目性和随机性。比如利用 GoogleHacking 原理不仅能批量查找具有已知漏洞的应用程序，还包括 SQL 批量注入和挂马等。但对于重要的 WEB 应用（比如运营商或金融），始终有受利益驱动的黑客进行持续的跟踪。

如果说传统的“大而全”安全防护产品能抵御大多数由工具产生的攻击行为，那么对于有针对性的攻击行为则力不从心。而 WAF 正是应需求而生的一款高端专业安全产品，这也是市场需求细化的必然趋势。但由于其部署和功能方面与 IPS 有类似，有人提出疑问，为什么不能用 IPS？或者说 WAF 与 IPS 有什么异同？谁更适合保护 WEB 服务器？

这些疑问其实是有道理的，差异化的产生在于高端需求是不同的，从而需要细化功能生产贴合具体需求和符合应用现状的产品，这也是用户需求随着业务自身发展所决定的。

保镖和保安

为了更好的理解两款产品的差异性，我们先用保镖（WAF）和保安（IPS）这个比喻来描述。

大楼保安需要对所有进出大楼人员进行检查，一旦发现可疑人员就禁止他入内，但

如果混进“貌似忠良”的坏人去撬保险柜等破坏行为，大楼保安是无能为力的。

私人保镖则是指高级别、更“贴身”的保护。他通常只保护特定的人员，所以事先需要理解被保护人的身份、习惯、喜好、作息、弱点等，因为被保护人的工作是需要去面对不同的人、去不同的场合，保镖的职责不能因为危险就阻止、改变他的行为，只能去预见可能的风险，然后量身定做合适的保护方案。

这两种角色的区别在于保安保护的是整个大楼，他不需要也无法知道谁是最需要保护的人，保镖则是明确了被保护对象名单，需要深刻理解被保护人的个性特点。

职业对比	被保护对象	站岗位置	分析方法	被突破防护后
保镖	老板	贴身式	根据老板性格、行程、弱点等分析日常接触人范围和行为	老板有防弹衣防止受伤
保安	大楼	大楼门口	所有进出大楼的人形迹，衣饰，表情，出入证判断	只能报警

通过上面的比喻，大家应该明白两者之所以会感觉相似是因为职责都是去保护，但差异在于职能定位的不同。从技术原理上则会根据定位来实现。下面通过几个层面来分析 WAF 和 IPS 的异同。

事件的时间轴

对于安全事件的发生，有三个时间点：事前、事中、事后。传统的 IPS 通常只对事中有效，也就是检查和防护攻击事件，其他两个时间点是 WAF 独有的。

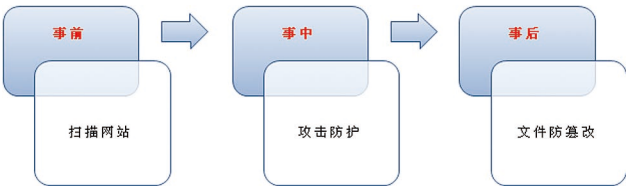


图 1.2 事件时间轴

如上图所示，事前是指能在事件发生之前通过主动扫描检测 WEB 服务器来发现漏洞，通过修复 WEB 服务器漏洞或在前端的防护设备上添加防护规则等积极主动手段来预防事件发生。事后则是指即使 WEB 服务器被攻击了，也必须有网页防篡改功能，让攻击者不能破坏网站数据。

为什么不能具备事中的 100% 防护能力？其实从以下几个方面分析，我们就能理解，对于事中只能做到相对最佳防护而不能绝对。

1. 软件先天是有缺陷的，包括应用到第三方的组件和函数库无法控制其安全性；

2. 应用程序在更新，业务是持续发展的、动态的，如果不持续监控和调整安全策略，也是会有疏漏的；

3. 攻击者永远在暗处，可以对业务系统跟踪研究，查找漏洞和防护缺陷，用各种变形繁杂的手法来探测，并用于攻击；

4. 任何防护设备都难以 100% 做到没有任何缺陷，无论是各种算法还是规则，都是把攻击影响降低到最小化。

所以需要用一个可闭环又可循环的方式去降低潜在的威胁，对于事中疏漏的攻击，可用事前的预发现和事后的弥补，形成环环相扣的动态安全防护。事前是用扫描方式主动检查网站并把结果形成新的防护规则增加到事中的防护策略中，而事后的防篡改可以保证即使疏漏也让攻击的步伐止于此，不能进一步修改和损坏网站文件，对于要求信誉高和完整性的用户来说，这是尤为重要的环节。

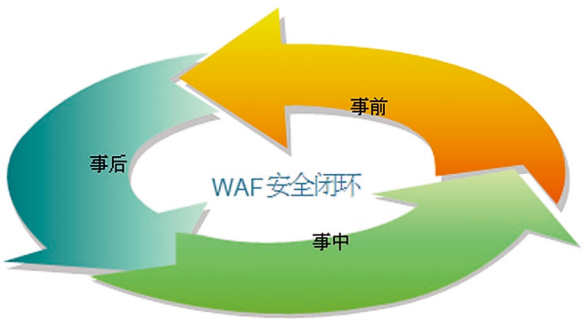


图 1.3 WAF 安全闭环

如果仅仅是对于事件的时间轴有区别，那么还是可以采用其他产品来进行辅助，但关键的是事中的防护也有深度的差异，下面我们来谈谈防护在事中的差异。

纵深度差异

事中，也就是实时防护，两者的区别在于一个是纵横度，一个是深度。IPS 凸显的优势在于纵横度，也就是对于网络中的所有流量进行监管，它面对的是海量数据，下图的 TCP/IP 模型中网络流量从物理层到应用层是逐层递交，IPS 主要定位在分析传输层和网络层的数据，而再往上则是复杂的各种应用层协议报文，WAF 则仅提供对 WEB 应用流量全部层面的监管。

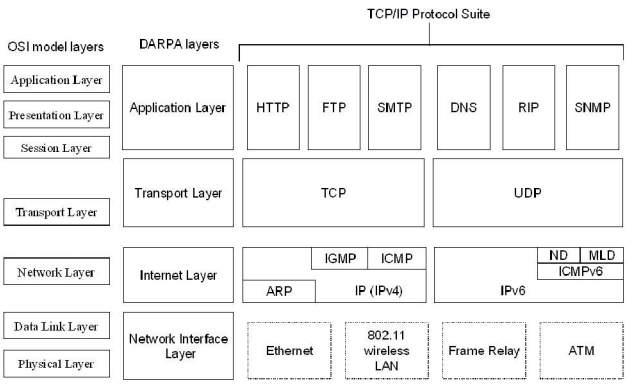


图 1.4 数据结构图

监管层面不同，如果面对同样的攻击，比如 SQL 注入，它们都是可以防护的，但防护的原理有区别，IPS 基本是依靠静态的签名进行识别，也就是攻击特征，这只是一种被动安全模型。如下是一个 Snort 的告警规则：

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"SQL Injection - Paranoid"; flow:to_server, established;uricontent:".asp";pcre:"/(\%27)|(\’)|(\-\-)|(%23)|(#)/i"; classtype:WEB-application-attack; sid:9099; rev:5;)

这里主要是检查在 SQL 注入中提交的元字符，包括单引号（‘）和双横（ -- ），从而避免注入’ 1 or 1=1— 之类的攻击发生，但同时又要考虑这些元字符转换成 Hex 值来逃脱过滤检查，于是又在规则

里增加了其对应的十六进制编码后的字符串。

当然，要从签名特征来识别攻击要考虑的东西还很多，不仅元字符还有 SQL 关键字，包括 :select insert update 等，以及这些关键字的大小写变形和拼接，利用注释逃脱过滤，如下所示 :

使用大小写混杂的字符 :SeLecT fRom”

把空格符替换为 TAB 符或回车符 :select[TAB]from

关键词之间使用多个空格 :select from

字符串的数值编码 :0x414141414141 或 0x41004100410041004100

插入被数据库忽略的注释串 :sel/**/ect fr/**/om select/**/ from

使用数据库支持的一些字符串转换功能 :char(65) 或 chr(65)

使用数据支持的字符串拼接操作 :'sel'+'ect '+'fr'+'om'” 、“'sel'||'ect '||'fr'||'om'

可以设想一下，如果要检测以上的变形字符后的攻击则需要增加相应的签名特征，但更重要的是要充分考虑转换编码的种类，上面示例的 snort 的规则把可疑字符以及其转换后的 Hex 值放入同一条规则里检查，如果对于变形后繁多的攻击种类，这是滞后的并且会造成签名臃肿。

产品架构

大家知道 IPS 和 WAF 通常是串联部署在 WEB 服务器前端，对于服务器和客户端都是透明的，不需要做任何配置，似乎都是一样的组网方式，其实有很大差异。首先我们看看市面主流 WAF 支持的部署方式 :

- 桥模式
- 路由模式
- 反向代理
- 旁路模式 (非串联)

这两者串联部署在 WEB 服务器前端时，市面上的大多数 IPS 均采用桥模式，而 WAF 是采用反向代理模式，IPS 需要处理网络中所有的流量，而 WAF 仅处理与 WEB 应用相关的协议，其他的给予转发，如下图 :

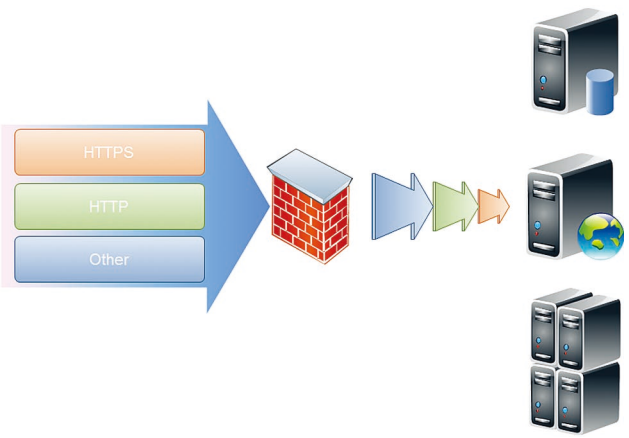


图 1.5 多协议图

桥模式和反向代理模式的差异在于 : 桥模式是基于网络层的包转发，基本都没有协议栈，或只能简单地模拟部分协议栈，分析网络报文流量是基于单包的方式，所以要处理分片报文、数据流重组、乱序报文、报文重传、丢包都不具备优势。同时网络流量中包括的

协议种类是非常多的，每种应用层协议都有自身独特的协议特征和格式要求，比如 Ftp、SSH、Telnet、SMTP 等，无法把各种应用流量放到应用层协议栈来处理。

绿盟科技 WAF 系统内嵌的协议栈是经过修改和优化的，能完全支持 Http 应用协议的处理，这意味着必须遵循 RFC 标准（Internet Requests For Comments）来处理 Http 报文，包括如下主要 RFC:

- RFC 2616 HTTP 协议语法的定义
- RFC 2396 URL 语法的定义
- RFC 2109 Cookie 是怎样工作的
- RFC 1867 HTTP 如何 POST，以及 POST 的格式

RFC 中对 Http 的 request 行长度、URL 长度、协议名称长度、头部值长度等都是有严格要求的，以及传输顺序和应用格式，比如 Html 参数的要求、Cookie 的版本和格式、文件上传的编码 multipart/form-data encoding 等，这些应用层内容只能在具有完整应用层协议栈的前提下才可正确识别和控制，对于不完整的丢包，重传包以及伪造的畸形包都会通过协议校验机制来处理。

上一节提到的 WAF 对 Https 的加解密和多重编码方式的解码正是由于报文必须经过应用层协议栈处理。反之，IPS 为什么做不到？是由于其自身的桥模式架构，把 Http 会话“打碎”成多个数据包在网络层分析，而不能完整地从应用层角度来处理和组合多个报文，并且应用层协议繁多，全部去支持也是不现实的，产品的定位并不需要这样。下一节的学习模式更是两者的截然不同的防护机制，而这一机制也是有赖于 WAF 的产品架构。

基于学习的主动模式

在前面谈到 IPS 的安全模型是应用了静态签名的被动模式，那么反之就是主动模式。WAF 的防御模型是两者都支持的，所谓主动模式在于 WAF 是一个有效验证输入的设备，所有数据流都被校验后再转发给服务器，能增加应用层逻辑组合的规则，更重要的是具备对 WEB 应用程序的主动学习功能。

学习功能包括：

1. 监控和学习进出的 WEB 流量，学习链接参数类型和长度、form 参数类型和长度等；

2. 爬虫功能，爬虫主动去分析整个 WEB 站点，并建立正常状态模型；

3. 扫描功能，主动去扫描并根据结果生成防护规则。

基于学习的主动模式目的是为了建立一个安全防护模型，一旦行为有差异则可以发现，比如隐藏的表单、限制型的 Listbox 值是否被篡改、输入的参数类型不合法等，这样在面对多变的攻击手法和未知的攻击类型时能依靠安全防护模型动态调整防护策略。

结尾

WAF 更多的特性，包括安全交付能力、基于 cache 的应用加速、挂马检查、抗 DDOS 攻击、符合 PCIDSS 的防泄密要求等都表明这是一款不仅能进行攻击防护，同时又能够在满足客户体验和机密数据防护要求的高度集成的专业产品。本文仅从产品特征的对比角度来分析 WAF 的部分技术原理，并没否定 IPS 的价值，毕竟两者在部署场景和功能上具有很大差异。

参考文献：

[1]. Hypertext Transfer Protocol -- HTTP/1.1 http://www.ietf.org/rfc/rfc2616.txt

[2]. HTTP State Management Mechanism http://www.ietf.org/rfc/rfc2109.txt

[3]. Form-based File Upload in HTML http://www.ietf.org/rfc/rfc1867.txt

[4]. Uniform Resource Identifiers (URI): Generic Syntax http://www.ietf.org/rfc/rfc2396.txt

[5]. Perl-compatible regular expressions (pcre) http://www.pcre.org

[6]. Advanced SQL Injection http://www.nextgenss.com/papers/advanced_sql_injection.pdf [7]. The Snort IDS http://www.snort.org

[8]. WEB Application Firewall Evaluation Criteria http://www.WEBappsec.org/projects/Wafec/v1/wasc-Wafec-v1.0.html

[9]. 绿盟 WEB 应用防火墙产品白皮书 http://www.nsfocus.com/1_solution/NSF-PROD-WAF-V6.0-WH.pdf

关联文章：

建议阅读下面关联文章，更好理解 WAF 和 IPS 的区别：

[1].《WEB application firewall 防护 WEB 攻击有天然优势》绿盟科技产品市场部 秦波

Fuzzing技术漫谈

研究部 刘业欣

摘要：近些年的 0day 漏洞绝大部分都是靠 Fuzzing 技术发现的，那么究竟什么是 Fuzzing 技术？Fuzzing 技术是如何工作的？Fuzzing 技术的未来发展如何将是本文要探讨的主要内容。

关键词：Fuzzing 漏洞挖掘 测试

一、什么是 Fuzzing 技术？

由于“Fuzzing”这个英文单词到目前为止还没有一个权威且准确的中文翻译，因此要搞清楚什么是 Fuzzing，首先需要明确几个英文单词的含义：

Fuzz:

“Fuzz”发音 [fʌz]，本义是细毛、绒毛的意思，作为动词的含义是成绒毛状或起毛，作为动词还有一个引申义是变模糊。在计算机领域里这个词的出现大部分都是使用其引申义。

Fuzzing:

“Fuzzing”是作为动词“Fuzz”的名词形式。这里也是变模糊的意思。

Fuzzer:

“Fuzzer”是对使用 Fuzzing 技术的工具的统称。

明确了以上单词的含义，只是帮助我们理解其字面意思，但从字面上还是不能理解 Fuzzing 技术的真实含义。所谓 Fuzzing 技术属于软件测试技术的一种，与一般软件测试技术的边界值分析 (BVA) 类似，但并不局限于边界值，而是所有可能导致问题的输入值（可以统称为畸形数据）。Fuzzing 技术突出对于大量测试用例采用自动化的方式去完成测试。Fuzzing 技术与一般软件测试技术关注的 Bug 类型不同，Fuzzing 技术只关注那些导致软件崩溃或者其他与漏洞相关的 Bug。因此 Fuzzing 技术成为漏洞挖掘的方法之一，也逐步成为了最流行的漏洞挖掘方法。传统的 Fuzzing 技术只是一种黑盒测试技术，即不关心软件的内部实现而只对外部接口进行测试。随着 Fuzzing 技术的发展，也逐步向白盒测试技术发展，即也要分析软件的内部流程，并内外结合最终成为灰盒测试技术。

Fuzzing 技术最早可以追溯到 1989 年，美国威斯康星州 (Wisconsin) 大学的 Barton Miller 教授及其团队为了测试 Unix 应用程序的健壮性开发了第一款 Fuzzing 测试工具。虽然这个 Fuzzing 测试工具还较为原始，但它已经具备了 Fuzzing 技术的核心理念。1999 年芬兰奥卢 (Oulu) 大学 PROTOS 团队开始开发各种协议和格式的测试用例集，这些测试用例集为协议和格式的 Fuzzing 测试

提供了基础的畸形数据。2000 年以后，随着各种 Fuzzing 框架工具的诞生，Fuzzing 技术也得到了快速发展。具有代表性的有 2002 年美国 Immunity 公司的 Dave Aitel 开发的 SPIKE 工具。SPIKE 以发现多个 Sun RPC 和微软 RPC 漏洞而著名，是开放源代码的针对网络协议的 Fuzzing 测试工具。还可以基于 SPIKE 框架开发针对新协议的 Fuzzing 测试功能。2004 年针对文件格式的 Fuzzing 测试工具开始大量出现，因为当年的微软安全公告 MS04-028 是一个关于处理 JPEG 文件格式导致的漏洞，人们开始意识到文件格式漏洞的重要性，此后包括微软 Office 在内的大量文件格式漏洞被发现。2005 年 Fuzzing 测试工具的商业产品陆续出现，代表性的有 Codenomicon 公司的 DEFENSICS、Mu Security(现为 Mu Dynamics) 公司的专用硬件产品和 Beyond Security 公司的 beSTORM。2006 年随着 Idefense 公司的 David Zimmer 开发的 ComRaider 和 Metasploit 公司的 H D Moore 开发的 AxMan 的推出，针对 ActiveX 接口的漏洞挖掘也广泛开展起来。ActiveX 漏洞数量随后也出现暴涨。2007 年 Google 公司的 Michal Zalewski 发布了一个革命性的 Fuzzing 工具 Bunny。Bunny 是通过修改 GCC 编译器，在编译阶段生成畸形输入数据，由于是在源代码基础上进行，因此可以做到完全的白盒测试。2009 年 BlackHat USA 大会上，德国柏林技术大学 (TU-Berlin) Collin Mulliner 和 Independent Security Evaluators 公司的 Charlie Miller 公布了在一些主流智能手机上对 SMS 漏洞挖掘的过程，标志着对嵌入式设备的 Fuzzing 测试即将流行。

二、Fuzzing 技术工作原理

Fuzzing 测试一般的过程如下：

确定测试目标

确定输入形式

生成畸形数据

执行被测目标

监控异常行为

确定漏洞利用

1、确定测试目标：

对某个产品以 Fuzzing 技术进行漏洞挖掘，那么就确定了这个产品为测试目标。测试目标的确定纯粹为漏洞挖掘者主观意识所决定。

2、确定输入形式

由于各种应用程序功能多样，因此输入形式有很多种，如文件、网络协议、COM/ActiveX 接口、API 接口等等。即使都是文件，还有二进制格式、文本格式、XML 格式等等。确定测试目标和输入形式之后，才可以选择合适的 Fuzzing 测试工具。

3、生成畸形数据

构造畸形的输入数据通常有下面几种方式：

1) 完全随机产生，也就是通常所说的盲 Fuzzing 测试 (Dumb Fuzzing)。采用这种方式可以做成一个通用的 Fuzzing 工具，但是由于针对性不强，漏洞挖掘的效率很低。

2) 在原有正常数据基础上进行修改。采用这种方式也可以做成一个通用的 Fuzzing 工具，虽然相比上面的方式针对性有所增强，但漏洞挖掘的效率仍然较低。

3) 根据输入数据格式自行构造畸形数据。采用这种方式必须要知道输入数据格式，Fuzzing 工具开发较为复杂，但针对性强，可以触发上面方式触发不了的漏洞。

当然几种方式结合才是最佳方式，依次用三种方式进行漏洞挖掘，逐步挖掘更深层次的漏洞。

4、执行被测目标

构造完畸形数据之后必须要把这些数据交给被测目标进行处理才能完成一次测试用例的测试任务。

5、监控异常行为

由于有大量的测试用例，并不是每一个测试用例都能触发漏洞，因此必须要有一个自动化的方式来监控被测目标，并且能够把发生异常的测试用例记录下来，以便事后分析。

6、确定漏洞利用

根据异常的记录信息来人为判断这个漏洞是否是可以利用的漏洞。判断方法可以结合静态分析和动态调试来综合判定。

三、Fuzzing 工具一览

开放源代码的 Fuzzing 工具：

通用	文件	网络协议	ActiveXCOM	WEB/HTML
Peach	FileFuzz	Sulley	ComRaider	MielieTool
SPIKE	FileH/FileP	Toaf	AxMan	WSFuzzer
Fuzzware	UFuz3	GFP	COMbust	RFuzz
zzuf		EFS	axfuzz	DOM-Hanoi
Bunny		QueRub	Dranzer	MangleMe

商业 Fuzzing 工具：

通用	文件	网络协议	ActiveXCOM	WEB/HTML
DEFENSICS		Mu Dynamics		
beSTORM				

Mu Dynamics 产品为网络协议 Fuzzing 的专用硬件产品。beSTORM 支持的测试类型最多。但这些商业产品在价格上都十分昂贵。

四、Fuzzing 技术局限性

虽然 Fuzzing 技术已经成为最流行的漏洞挖掘技术，但是 Fuzzing 技术不是万能，有它天生的局限性。通过 Fuzzing 技术挖掘的漏洞大多是传统的溢出类型漏洞，对于如鉴权绕过、后门等等这样的逻辑设计上的漏洞就显得力不从心了。多条件触发的漏洞，通

过单纯的 Fuzzing 技术也很难被发现。目前 Fuzzing 技术的弱项还不能够保证畸形输入数据能够覆盖到所有的分支代码，这样就会失去一些漏洞被发现的机会。因此往往使用通用性的 Fuzzing 工具的漏洞挖掘效率较低，如果要提高漏洞挖掘效率就需要漏洞挖掘者单独写针对性的 Fuzzing 代码，但这又有赖于漏洞挖掘者自身对格式或协议的理解以及漏洞类型的了解程度。

五、Fuzzing 技术展望

如何提高漏洞挖掘效率是目前 Fuzzing 技术发展的主要方向。漏洞挖掘效率可以从很多方面去提高：

1、增强输入数据的针对性

结合白盒测试技术（如果存在源代码可以直接利用源码；如果没有源代码可以结合逆向工程的反汇编或反编译结果）对代码流程进行分析并结合数据流分析和测试结果反馈分析完成以下目标：

1）减少测试用例的数量

2）提高代码覆盖率，争取做到全覆盖

2、采用并行和分布式技术

虽然可以减少测试用例的数量，但其绝对值还是巨大的，因此需要采用并行和分布式技术来加速执行，提高执行效率。

3、提高自动化能力可以完全替代人的操作

更多图形化的程序需要与用户交互才能进入某个代码流程，因此需要 Fuzzing 测试工具可以模拟人的行为，如键盘和鼠标的操作来完全自动的完成一个测试用例任务。

4、更多平台的支持

当前更多的 Fuzzing 工具还局限于桌面操作系统上，对于智能手机这样的嵌入式操作系统还需要进一步的支持，以方便挖掘更多的嵌入设备的漏洞。

5、更智能的 Fuzzing

能够自动识别更多的格式和协议类型，能够识别和处理更复杂的程序流程和异常行为。

参考资料

[1] Fuzzing: Brute Force Vulnerability Discovery, Michael Sutton, Adam Greene, Pedram Amini

[2] Demystifying Fuzzers, Michael Eddington

信誉系统应对新兴网络安全威胁

行业营销中心 卢小海

摘要：为应对安全威胁和攻击方法的迅速增长，绿盟科技定期对互联网相关站点进行威胁分析和信誉评级，累积 IP 地址、域名和 URL 等不同资源的内容和行为记录。同时，我们汇集来自于授权客户和第三方合作伙伴的威胁反馈、自身安全产品的安全事件以及安全研究团队的风险预警，与目标站点的历史信息进行整合，建立针对互联网领域的长期信誉追踪机制。互联网相关产品可以通过我们提供的开放信誉服务接口，对互联网资源的安全信誉进行实时查询；以其信誉评级作为判断依据，进行针对性的防护动作，以保护互联网终端用户。

关键词：互联网 信誉系统 云安全 挂马 恶意代码

随着 IT 产业的飞速发展和互联网用户数量的逐渐增加，互联网与人们工作和生活的结合更加紧密，依托互联网开展的商业活动也日益丰富。而与此同时攻击者也更为关注互联网，发展形成了具有相当规模的，针对安全威胁研究、生产和分发的“地下产业链”。这些攻击者利用恶意代码、垃圾邮件、钓鱼站点等不同攻击方法，给企业和个人造成财产损失、信息泄漏和信誉受损等不良影响。如何保护自己的用户使其免受互联网安全威胁的影响，已成为整个互联网相关硬件、软件、服务和网络提供商面临的共同挑战。

随着“地下产业链”不断扩张，层出不穷的安全威胁不断涌现。攻击者只需要少许的变化就可以产生全新的恶意代码，而基于传统特征库的防护者，需要耗费大量的时间和精力，对恶意代码样本进行采集、提取和分析；恶意代码分析和特征库分发的响应速度，只能大大滞后于攻击者产生和传播新恶意代码的速度，致使基于传统特征库的防护方法逐渐陷入困境。越来越大的特征库、越来越慢的扫描速度已经成为现有防护体系需要面对的难题。

为应对安全威胁和攻击方法的迅速增长，我们定期对互联网相关站点进行威胁分析和信誉评级，累积 IP 地址、域名和 URL 等不同资源的内容和行为记录。同时，我们汇集来自于授权客户和第三方合作伙伴的威胁反馈、自身安全产品的安全事件以及安全研究团队的风险预警，与目标站点的历史信息进行整合，建立针对互联网领域的长期信誉追踪机制。互联网相关产品可以通过我们提供的开放信誉服务接口，对互联网资源的安全信誉进行实时查询；以其信誉评级作为判断依据，进行针对性的防护动作，以保护互联网终端用户。

对传统安全防护体系来说，信誉系统是有力的补充。

随着互联网应用的重要性逐渐提升，安全威胁来源开始从传统的网络和系统层，转向以恶意代码为代表的应用层。仅仅 2008 年上半年，国内发现的恶意代码样本数量就超过了之前五年时间的总数，达到惊人的 900 万种。

由于攻击方式的研究不断成熟和深入，攻击者产生和传播恶意代码的成本日益降低；而防护产品仍然依赖于传统的样本采集和分析，特征码生成和分发机制。恶意代码样本数量的爆发式增长，直接导致传统的依赖于特征库的现有防护体系不堪重负。无论是特征库容量还是威胁响应速度，都难以跟上恶意代码的迅速增长。

为应对这个挑战，绿盟科技投入大量的网络和计算资源，对互联网资源（域名、IP地址、URL 等等）进行威胁分析和信誉评级。互联网产品只需针对目标资源向安全信誉服务查询，就可以获得相应的安全信誉评级信息；进而根据结果调整自身的防护策略，在恶意代码下载到本地之前，阻止客户端对恶意资源的访问，从而实现对客户端的保护。

为应对新兴安全威胁，信誉系统可以提供及时有效的检测和防护。

随着互联网应用的多样性不断发展，挂马网站、网络钓鱼、流氓软件等各种新的安全威胁也不断涌现。这些新兴攻击手法利用互联网用户的疏忽大意（网络钓鱼），以及对第三方的信任（挂马网站、垃圾邮件和IM）诱骗互联网用户并最终造成损失。

这种混搭多种攻击手法的安全威胁，通过把功能拆分到多个动作，以逃避面向行为进行防护的安全监控。面对这些新型的攻击方式，传统的基于已知特征的针对动作的防护体系，很难为互联网用户提供有效的防护。

信誉系统可以利用海量的计算资源分析从不同信息源获取的事件，并结合来自不同用户和合作伙伴的反馈进行关联；互联网用户仅需要通过简单的接口进行查询，即可获得相应的信誉评级进行防护。进而通过多来源、多维度信息的综合分析，解决从单一层面来解决新威胁的技术难题，建立针对各种新兴威胁的防护机制。

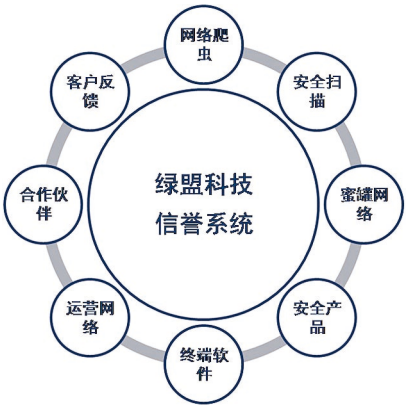
信誉系统并非一个孤立的系统，而是一个动态的由不同合作伙伴组成的生态系统。

随着互联网应用的适用面日益广泛，安全作为一种硬性的需求，被列入各种互联网产品和应用的考虑范畴中。而日新月异的攻击手法，也使得安全威胁的发现和防护，是一个立体的多层面的工作，不再是一两家安全公司能够完整覆盖。

现有传统安全体系往往是由厂商独立建立和维护，服务于自身产品和客户的封闭系统；臃肿的检测和防护模块，也难以被集成到第三方产品和应用中；此外冗长的法律和商务谈判，也使潜在合作者望而却步。

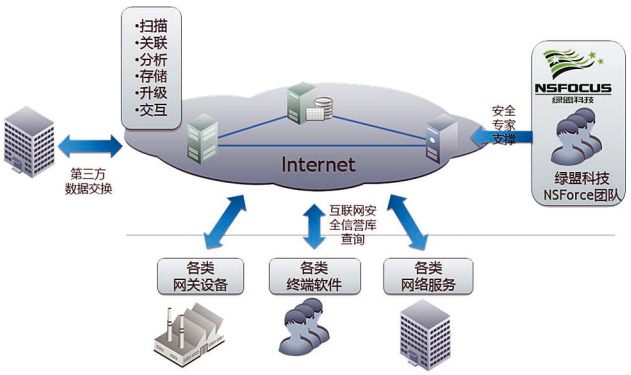
而基于安全信誉服务的轻量级客户端不再需要复杂的内容扫描和监控模块，只需要通过简单接口即可完成客户端的防护工作，大大减轻了进行集成的成本。绿盟科技会提供持续和稳定的服务端运维支持，通过汇集客户端实时反馈与合作伙伴的交换信息，进而改善服务的自身质量。整个信誉系统是为一个开放生态系统而设计，来源于互联网并服务于互联网。

在对自有产品提供支持的同时，信誉系



统也通过信誉服务为第三方产品和应用提供服务，使用者将通过双向信息反馈通道与信誉系统形成互动。

信誉系统自身是一个综合不同维度信息的知识库，通过扫描系统和反馈系统实时更新和积累原始数据。为提高发现威胁的及时性，信誉系统包含了一整套自动化闭环反馈处理流程，对客户反馈、合作伙伴和运营商提供的信息进行处理。



互联网企业或用户可以通过绿盟科技提供的开放接口，通过信誉服务进行查询。各种网关产品、终端软件和应用服务，可以在用户访问互联网资源前，通过对资源安全信誉进行查询，发现潜在的安全分析，一旦发现用户访问的互联网资源安全信誉存在问题，即可暂时停止用户对此资源的访问，从而达到保护用户的目的。

在与现有安全防护体系进行整合，结合主动探测和客户反馈之后，信誉系统可以更好地服务于整个安全体系中的合作伙伴，持续改善使用者的用户体验。

基于信誉库的互联网安全

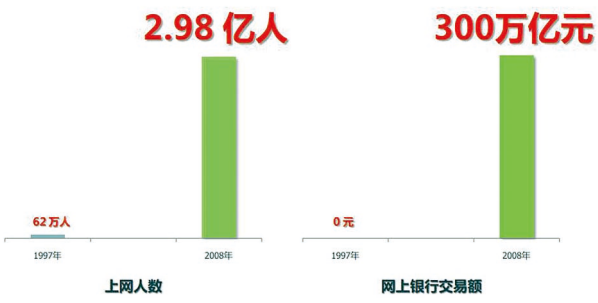
行业营销中心 李钠

摘要：本文从互联网安全的重要性谈起，概述了绿盟科技在互联网安全领域的规划与产品，详细介绍了绿盟科技基于信誉库的互联网安全解决方案。

关键词：互联网安全 信誉库 WEB 安全平台

互联网安全的重要性

从1987 年 9 月 20 日中国发出第一封电子邮件开始，中国正式开进入了互联网时代。而从 1997 年开始，互联网逐渐成为了中国人大众生活的一部分。据中国互联网络信息中心发布的 2008 年《中国互联网络发展状况统计报告》称，中国互联网使用者人数已经从 1997 年的 62 万人上升到 2.98 亿人，达到 1997 年的 481 倍。而据中国银行业监督管理委员会发布的《2008 年度银行业改进服务情况报告》称，中国网上银行交易额已经达到了 300 万亿元。由此可见，互联网已经成为人们日常生活中最重要的信息交换场所，而且越来越多的人习惯于通过互联网进行交易。

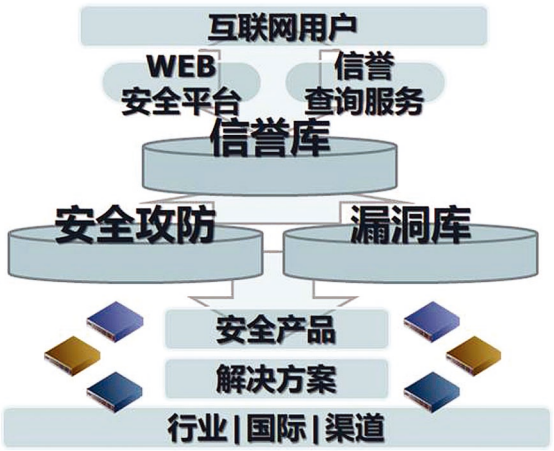


正是在这样的背景下，越来越多的攻击者将眼光投向了互联网，并且已经从简单的炫耀和展示能力的攻击行为转向了以牟利为主的攻击行为，并且形成了分工明确的“黑色产业链”。据中国国家计算机网络应急技术处理协调中心 CNCERT 透漏，2008 年“黑色产业链”年产值已经达到 76 亿元。

绿盟科技与互联网安全

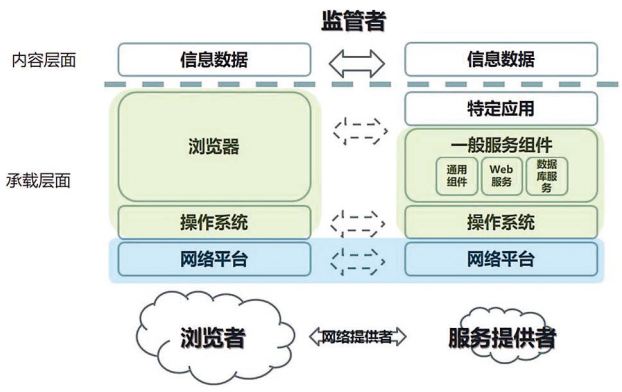
绿盟科技从成立之初就开始关注互联网的安全趋势，对安全攻防与漏洞库进行了持续高质量的研究工作。基于自身安全攻防和漏洞库方面近十年的积累，形成了一系列的安全产品和解决方案，并且通过行业、国际和分销渠道协助用户解决安全问题。

随着互联网的发展，越来越多的人、越来越多的业务将与互联网结合得越来越紧密，互联网相关的安全问题也将越来越明显的凸现。以往由厂商单向传递到用户的机制已经跟不上互联网的步伐。一方面为了更好地解决互联网上的安全问题，另一方面为了更及时地通过安全产品和解决方案解决用户遇到的互联网相关安全威胁，绿盟科技开始通过互联网提供基于信誉库的安全解决方案。

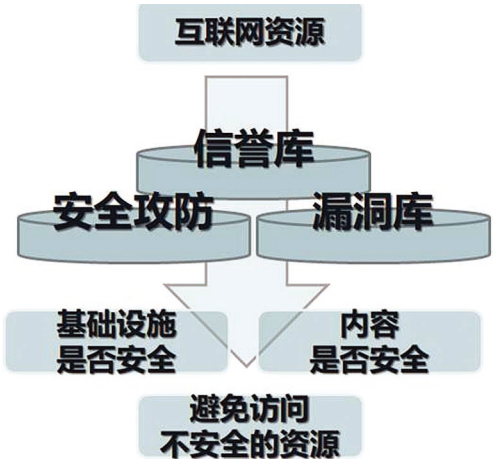


目前，绿盟科技主要通过 WEB 安全平台（WSP:WEB Security Platform）和信誉查询服务（RS:Reputation Service）对外提供服务。

绿盟科技基于信誉库的互联网安全解决方案



互联网不同的参与者对承载层面、内容层面都有相应的安全需求。如何解决好这些不同层次的安全需求，是互联网安全必需考虑的问题。目前绿盟科技推出的基于信誉库的互联网安全解决方案正是为了简化这样的问题而提出的。在这样的架构下，绿盟科技通过自身信誉库、安全攻防和漏洞库的积累，对于任何的互联网资源，绿盟科技都能对其内容是否安全，以及基础设施是否安全进行相应的评分。用户通过这样的评分机制能够避免访问到不安全、不可信的互联网资源，从而避免遭受损失。



绿盟科技 WEB 安全平台

目前，绿盟科技的 WEB 安全平台即将推出。此平台主要通过自服务的方式向网站所有者提供安全扫描类服务。

通过绿盟科技 WEB 安全平台，网站所有者可以对自身网站进

行一系列监控（目前主要包括安全漏洞、挂马等信息）。网站所有者可以通过自服务的方式调整自身网站的监控策略，从而实现对网站安全信息的及时了解。

绿盟科技 WEB 安全平台一旦发现安全漏洞或者网站页面被挂马，WEB 安全平台将通过多种方式通知用户及时进行处理。

绿盟科技荣获“政府网站安全产品优秀解决方案奖”

12 月 17 日，“2009 中国政府网站绩效评估与第四届中国特色政府网站评选结果发布大会”在北京梅地亚中心举行。会上，绿盟科技首次披露《2009 年政府网站挂马监测研究报告》部分数据，报告显示，政府网站安全形势依然严峻，目前我国政府网站绩效评估体系设计上存在安全指标的缺失，并没有考虑到网站安全问题给政府形象、政务网站业务运行带来的潜在风险与隐患。针对此情况，绿盟科技政府行业营销总监孙铁详细讲解了政府网站整体安全保障解决方案，并介绍了 WEB 安全监控平台的功能，希望通过政府网站安全评估服务，以评促建，帮助政府网站提前发现安全漏洞，避免网页挂马；即时发现安全漏洞，防患于未然。

目前，中国已经成为世界上网民最多的国家。在网络日益普及的今天，网站在发布信息方面的优势越来越明显。我国政府在“政务公开”政策的施行方式中，政府网站已经成为政府联系大众和企业的重要纽带。政府网站除信息发布之外，还承担着直接对外提供服务的重要职能，在不久的将来，企业和个人与政府“打交道”的理想方式，将是“基于网络的一站式服务”。

但是，在这样一个政府网站越来越重要、越来越普及的背景下，我国政府网站的安全形势却不容乐观：网站业务应用还存在着诸多安全隐患；政府网站绩效评估体系指标中缺乏安全指标的考量。孙铁在会上以“政府网站安全绩效评估与安全防护”为主题的

演讲中发布了绿盟科技最新的政府网站挂马数据监测研究报告，报告指出：在 2009 年 5 月到 12 月期间，绿盟科技共监测近 6 万多个网站（含部分二级域名），发现挂马网站数 175 个，挂马网站比例为千分之二点六；统计范围内的被挂马政府网站平均被挂马 3 次，平均挂马时间 214 小时。

2009 年 1 月至 10 月期间，某部信息中心委托国脉互联组织了《2009 年度全国某部省级行政主管部门网站绩效评估》工作，绿盟科技应邀参与网站绩效评估体系中的安全指标标准制定与具体的监测。分析结果表明，高达 68% 的网站存在不同程度的安全隐患问题，16% 的网站存在极高风险漏洞，在网站安全监测过程中，存在被攻击者在网站中插入恶意代码（通称“网站挂马”）的情况。即使在此次网站综合评分排名靠前的一些优秀省级网站，也有个别网站存在严重的安全问题。

政府门户网站作为政府与民众联系的窗口，网站的安全性已经是迫在眉睫。为此，绿盟科技在网站整体解决方案的基础上特推出互联网网站安全评估服务，帮助政府提前

发现安全漏洞，避免网页挂马；即时发现安全漏洞，防患于未然。孙铁强调，“绿盟科技网站安全监控平台主要有三大功能：风险评估及漏洞管理功能、挂马检测功能、安全预警功能”。他进一步解释，“绿盟科技网站安全监控平台可以对本地主机、WEB 服务器、域名等进行安全评估和漏洞检测，做出一整套全面解决方案的集合，用于帮助政府信息管理部门侦测、描述和改善政府网站正面临的各种安全风险。总而言之就是将漏洞扫描、漏洞管理、漏洞修补、关联系统的安全日志集于一身，最后以安全评估报告的方式展现给政府信息管理与维护部门”。

最后，孙铁还从合规性和 WEB 应用安全防护两个角度进一步诠释了绿盟科技政府门户网站的整体安全保障解决方案，从而做到事前预警，事中防护，事后恢复、监控，最终全方位地保障政府网站安全。在本次大会上，绿盟科技荣获政府网站安全产品优秀解决方案奖。

工信部软件服务业司赵小凡司长莅临绿盟科技参观调研

12 月 16 日，工业与信息化部软件服务业司赵小凡司长一行来到绿盟科技参观调研。赵司长此次调研的目的是了解国内信息安全企业经营发展状况，了解信息安全行业的新技术、产品、服务和应用的发展趋势，交流研讨信息安全产业发展的问题和对策。绿盟科技作为国内信息安全行业的领先代表企业，成为赵司长此次行业调研的第一站。陪同参观调研的还有工信部软件服务业司软件产业处孙文龙处长、信息服务业处尹洪涛处长、北京市经信委软件与信息服务业处姜广智处长以及工信部相关支撑单位的人员。

在座谈过程中，沈总介绍了公司的基本情况、生产经营、技术研发、国际拓展以及企业未来发展规划等方面的情况，同时，沈总还深刻分析了国内信息安全产业的现状以及成因，并与工信部领导展开交流。

赵司长对绿盟科技在生产经营各方面所取得的优异业绩给予充分肯定，对公司扎实研发、国际化拓展以及近些年取得的成绩表示赞赏。对公司发展十年并越做越好的成长历程给予了高度评价。

赵司长指出，绿盟科技作为国家信息安全行业的重点企业，为产业的发展起到了积极的推动作用。面对激烈的市场竞争，绿盟科技要进一步加大人才培养和科技投入，依靠技术创新，进一步提高研发和产品质量水平，提升企业的核心竞争力。同时，也要抓住国家政策指导、政府帮助的机遇，更好的发挥优势、释放潜能、做大做强，为国家信息安全产业做出大贡献。

随后，沈总陪同赵司长一行参观了公司产品、研发、生产、办公环境等，对公司整体情况有了更进一步的了解。

绿盟科技出席第七届网络管理技术大会并连获四项大奖

12 月 10 日，由中国电子信息产业发展研究院（赛迪集团）主办、《网管员世界》杂志社承办的 2009 年第七届网络管理技术大会在北京世纪金源大饭店召开。在今年的网络管理技术大会上，绿盟科技凭借雄厚的技术实力和卓越的产品性能，再次一举获得 2009 中国 IT 运维与管理信息安全首选提供商、2009 中国网络技术与产品调查网管员最喜爱的IPS产品奖、WEB应用安全产品奖、安全审计产品奖共四个奖项。

会上，主办方分享了 2009 中国网络技术调查结果，结果显示，目前对于网络的稳定性和安全性的需求高居榜首。对于安全运维管理内容的需求，30% 的企业选择了安全评估，33% 的企业选择了漏洞，安全加固占 11%，其他占 4%。针对调查中关注度很高的 WEB 应用安全，绿盟科技产品市场部秦波以“如何降低网站风险”为主题，从技术层面对 WEB 应用安全进行了深刻剖析。他首先从宏观角度分析了 WEB 安全问题的本质和根源，并通过解读和运用 OWASP 新的 2010 版 TOP10 进而分析如何选择合适的 WAF 产品，WEB 应用安全需要解决哪些问题来降低风险，保障 WEB 业务系统运行。他指出，一个优秀的 WAF 产品是应该可以应付不同类型、不同难度的攻击行为。本次活动，与会代表还就目前企业在 IT 运维方面的问题、如何更好地提升IT运维水平、提高 IT 运维效率等一些热点话题和与会的网络主管人员进行了交流与讨论。

绿盟科技参加第三届移动互联网大会—畅谈云安全

12 月 8—9 日，由中国移动主办、中国移动研究院承办的第三届移动互联网大会在北京国际会议中心隆重开幕。作为行业内有巨大影响力的技术盛会之一，本届大会以“无处不在的网络，无所不能的业务”为主题，吸引了来自行业主管部门、电信运营商、研究机构、通信信息设备企业、增值服务与技术开发商的代表和专家听众 2000 多人参加。

绿盟科技应邀参展，技术经理万慧星在云计算分论坛做了“安全漫步云中”的精彩演讲。

万慧星主要围绕互联网安全的新形势、互联网安全建设的新思路，以及云安全为运营商带来的新机遇等 3 个方面畅谈对于云安全的理解。他指出，“互联网在各个层面的价值体现，带来了利益焦点的转移，利益从实体经济转移到虚拟经济。正是由于这些价值利益的转移，也产生了一些新兴的攻击方法，给互联网安全带来了新的威胁。”在互联网的商业模式下，仅仅依靠传统的安全方法还不能完全满足安全的需求。因此我们需要一些新的方法；需要信誉机制，需要基于 WEB 域名、身份等信誉机制；我们还需要关联分析、挖掘引擎等等来处理越来越多的新型安全问题。而利用云安全来实现这些目标是一个很好的思路。“我们看到云计算已经成为互联网未来的发展方向，运营商可以利用大量 IDC 计算资源为个人、中小企业用户提供更为丰富的业务应用。同时，云安全是云计算非常好的一种应用，也存在着大量的用户需求。可以基于云安全平台，为互联网用户、移动互联网用户提供在线安全扫描、流量清洗、WEB 过滤、终端安全、安全存储等安全业务。”

在本届互联网大会上，云计算与云安全受到了前所未有的关注，会场挤满了前来听讲的听众，气氛热烈。来自运营商、网络厂商、安全厂商的代表从各自的领域畅谈了对于云计算、云安全的理解。从观点到模式、从尝试到实践，云计算、云安全的概念正在付诸于产业链各个环节的实际行动中。

绿盟科技出席“电力信息安全与蝴蝶效应”VIP 沙龙

11 月 21 日，由中国电力企业联合会所属《中国电力企业管理》编辑部举办的“电力信息化 VIP 俱乐部”沙龙在北京拉斐特城堡召开。参加本次沙龙的单位包括：国家电网公司、中国电科院信息安全研究所，以及来自华能集团、大唐集团、中电投集团、华电集团、神华集团、国华集团的多位信息化资深专家及领导。绿盟科技能源行业团队在吴云坤副总裁率领下，应邀出席了沙龙并做了主题演讲。

本期沙龙主题为“信息安全与蝴蝶效应”。绿盟科技能源行业顾问张书嘉发表了《基线式安全与蝴蝶效应—论电力信息安全的持续测量、多维保障与运维绩效》的主题演讲，演讲从“安全水平的持续测量与补偿、基线式的安全配平与决策支撑、以及基线安全理论对于电力系统的实践可行性”等方面论述了诸多电力安全建设的焦点问题。近距离剖析了电力系统的事前短板、新的安全保障与运维绩效思路，获得了与会专家的一致好评。会后，绿盟科技应邀参与了“电力双网安全隔离的方案可行性与收益”主题辩论会，并从内容威胁、入侵途径、运维绩效等方面论述了辩方观点，获得评委专家的一致好评。通过此次活动，绿盟科技展示了最新的行业研究成果与解决方案，并面向电力行业的资深专家作了汇报，得到了更多的来自行业专家的指导和认同；同时也提升了绿盟品牌在

电力行业的成熟度，完善了绿盟科技面向电力行业的客户服务能力。

绿盟科技荣获 2009 年中国“十大金融科技杰出企业”奖

11 月 26 日，“2009 年度中国金融科技发展论坛”在北京召开。来自中国人民银行、工业与信息化部、中国银行业监督管理委员会、中国保险业监督管理委员会，其他部分中央部委、中国科学院研究生院金融创新中心，以及数十家银行、证券、保险等领域的信息科技工作者、IT 专家约 200 余人出席了本次论坛。绿盟科技在本次盛会上荣获 2009 年度中国“十大金融科技杰出企业”奖。《中国金融科技发展论坛》举办至今，国际经济和金融形势都发生了重大变化，尤其是这次全球范围的金融风暴更是触及了多个领域，使我国金融行业受到了不可避免的影响。为此，本届论坛上，与会嘉宾以“金融危机下的 IT 治理”为主题进行了热烈的探讨。

开展 IT 治理是金融市场不断发展的必然产物，而 IT 治理的结果又将进一步推动金融市场的健康发展，尤其是在全球金融危机的大背景下，IT 治理显得尤为重要。为此，中国银监会信息中心处长骆絮飞、中国保监会信息中心规划处长李春亮分别以《银行业 IT 治理与信息科技管理》、《中国保险业信息化现状及发展展望》为主题做了精彩演讲。

中国金融科技发展论坛始终以“推动金融业的繁荣与发展”为宗旨，为国内外关注金融领域的单位和个人提供高层次、高品质的交流平台，同时奖励为中国金融业信息化建设及金融风险防范方面做出突出贡献的优秀企业、企业人才及客户信赖的产品。本届论坛评出了“十大金融科技杰出人物”、“十大金融科技企业杰出人物”、“十大金融科技杰出企业”、“十大金融科技企业用户信赖产品”四个奖项，并在论坛期间举行了颁奖典礼。绿盟科技与英特尔、日立等公司一起，荣膺“十大金融科技杰出企业”奖。

本次论坛由中国银河证券副总裁陈静主持，绿盟科技副总裁郭晓鹏、金融行业销售总监郝东林、金融行业顾问徐一丁、北京分公司孙惟皓参加了本次论坛，并与各位专家进行了深入的探讨与交流。

人力资源和社会保障部信息中心感谢绿盟科技保障通信安全


人力资源和社会保障部信息中心

感 谢 信

人力资源和社会保障部 2010 年度国家机关及其直属机构考试录用公务员网上报名工作，已于 10 月 26 日圆满完成。作为此次负责网上报名通信安全保障工作的绿盟科技，日前收到了来自人力资源和社会保障部信息中心的感谢信。

信中写道：“从工作准备期到圆满完成，绿盟科技参与网络安全保障工作的员工提供了热情、细致、专业、及时、优质的技术服务，展现出良好的企业风范及辛勤付出的职业精神。”，对绿盟科技的工作表示衷心感谢。

为了保障 2010 年度国家机关及其直属机构考试录用公务员工作的顺利进行，绿盟科技在准备期协助用户多次进行内部攻击测试，优化网络部署及设备配置；考试期间，通过 7*24 小时职守实时观测、记录网络流量为预警提供了有效数据，并多次参与处理应急事件，最终确保网络的畅通。

绿盟科技以绝对优势继续领跑国内 IPS 市场

国际权威咨询公司 IDC 发布的 2009 年上半年中国 IT 安全市场份额数据显示，绿盟科技凭借绝对领先的产品市场份额优势，再次成为入侵检测 / 防御硬件市场的领导者，这是继荣获 Frost&Sullivan 授予的国际奖项之后，绿盟科技产品市场领导力的又一有力证明。

IDC 公布的《中国 IT 安全硬件市场分析与预测，2009-2013（2009 上半年）》报告指出，尽管受金融危机的影响，部分中小型企业减缓了 IT 投资，但中国 IT 安全硬件市场在 2009 年上半年仍保持了 10.5% 的同比增长速度，IT 安全营收好过预期。

入侵防御硬件市场仍然是各个厂商重点拓展的领域，该市场在 2009 年上半年同比增长 9.1%，市场规模达到 US$24.8M，而且第一次超过了入侵检测硬件市场的同期规模。入侵检测硬件市场表现疲软，再次成为国内惟一出现负增长的硬件市场，2009 年上半年同比减少 5.9%，市场规模为 US$21.6M，IDC 预计下半年该市场的规模与去年基本持平。

作为国内安全企业的领导者，绿盟科技的“绿盟 NIPS”和“绿盟 NIDS”在今年上半年的市场表现都很抢眼，其中“绿盟 NIPS”凭借其 20.8% 的市场占比一举超越国际主流 NIPS 产品，以领先第二名 8.5% 的绝对优势重回榜首。面对逐渐萎缩的入侵检测硬件市场，“绿盟 NIDS”也保持了强劲的增长势头，产品营收较去年同期有较大幅度的增长，继续领跑国内市场。未来，绿盟科技将持续加大在 NIPS/NIDS 市场的投入，为广大用户提供更加优质的产品和服务。

绿盟科技荣获“中国电信业激情 60 年十大行业杰出贡献企业”奖

10 月 29 日—31 日，作为中国信息通信产业的高峰盛会，第八届中国信息港论坛在青岛如期举行。本次论坛为庆祝建国 60 周年，特举行《记录中国电信业的光荣与梦想主题颁奖盛典》活动，绿盟科技荣获“中国电信业激情 60 年十大行业杰出贡献企业”奖。

中国信息港论坛”作为通信业界一年一度的“财富论坛”，一直以来，深得国内运营商和电信制造商的认可，对推动我国通信运营业面向信息化、推广信息化应用发挥了重要作用。论坛举办期间，众多国内外电信运营和通信信息服务企业高层与全球 IT 知名专家学者共同探讨通信业信息化的最新动向。

本届论坛，为表彰建国 60 年以来在电信及 IT 领域对国家、行业以及社会有过突出贡献和影响力的企业，根据《中国电信业激情 60 年—风采企业奖评选办法》，经相关单位申报，组委会审核通过，评选出“十大光纤光缆企业”、“十大网络服务提供商”、“十大行业杰出贡献企业”。在此项评选中，绿盟科技被授予“十大行业杰出贡献企业”。

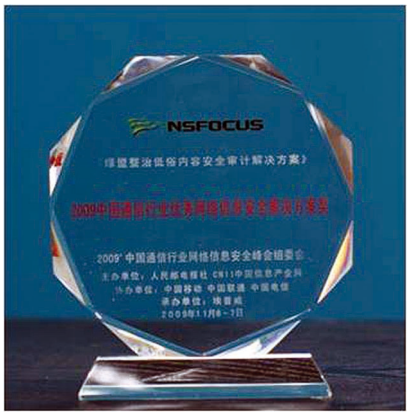
绿盟科技作为国内安全企业的领导者，一直以“巨人背后的专家”为己任，致力于网络安全事业。经过近十年的快速发展，已成长为面向国际市场的企业级网络安全解决方案供应商。为政府、运营商、金融、能源等各大行业的用户提供覆盖脆弱性风险评估和管理、入侵检测和防护、拒绝服务攻击防护、企业内网终端安全等多个领域的防护能力。

绿盟科技参加 2009 中国通信行业网络信息安全峰会

随着 3G 与全业务运营的进一步发展，网络信息安全对于通信行业的重要性和紧迫性越发突出。11 月 6—7 日，由人民邮电报社、CNII 中国信息产业网、埃普威公司共同举办的 2009 第四届中国通信行业网络信息安全

峰会如期举行。绿盟科技应邀出席，并在会上就“运营商门户网站安全防护思路”、“云安全的挑战与机遇”两个话题做了主题演讲，赢得了与会者的广泛好评。绿盟科技的《绿盟整治低俗内容安全审计解决方案》、《绿盟运营商门户网站安全解决方案》也获得了本次峰会运营商专家评选并颁发的“2009 中国通信行业网络信息安全优秀解决方案”奖。

绿盟科技行业营销中心田民首先从案例入手形象地阐述了目前门户网站所面临的安全风险，并结合门户网站的特性深刻剖析了门户网站生命周期各阶段所面临的问题，最后重点提出了解决门户网站安全问题的思路和方案。他指出，“价值是门户网站防护的核心，这个价值一方面是运营商价值的维护；另一方面还包括最终用户价值的维护。”同



绿盟整治低俗内容安全审计解决方案

绿盟运营商门户网站安全解决方案

时，他还就绿盟科技门户网站安全防护的新思路—云安全做了解读。在“云安全的挑战与机遇”的主题演讲中，绿盟科技行业营销中心卢小海围绕云安全所面临的挑战以及新的计算模式下绿盟科技对云安全的一些思考做了详细而深刻的诠释。

网络无所不在，安全威胁无处不在，解决方案的探讨一贯是通信安全峰会的着力点。本届峰会分为“网络安全保障 3G 与全业务运营”、“运营商信息安全服务与技术支撑”、“省运营商网络安全思考与实践”、“通信行业网络安全管理与促进交流”、“2009 通信行业应用安全”等 5 个主题峰会。与会嘉宾围绕 2009 通信行业网络信息安全最新趋势，结合主题峰会内容分享了各自的最新实践。

绿盟远程安全评估系统与绿盟 WEB 应用防护系统双双获得 EAL3 级证书

10 月 28 日，绿盟科技自主研发的“绿盟远程安全评估系统”、“绿盟 WEB 应用防护系统”双双获得由中国信息安全测评中心颁发的“国家信息安全测评信息技术产品安全测评证书（EAL3 级）”。作为国内漏洞扫描产品及 WEB 应用安全产品的领跑者，绿盟科技是首家也是目前惟一一家获得该类产品 EAL3 级证书的厂商。

据悉，信息安全产品分级评估是中


国家信息安全测评
信息技术产品安全测评证书
级 别：EAL3
绿盟远程安全评估系统 V6.0

国信息安全测评中心依据国家标准 GB/T 18336—2001，综合考虑产品的预期应用环境，通过对信息安全产品的整个生命周期，包括技术、开发、管理、交付等部分进行全面的安全性评估和测试，验证产品的保密性、完整性和可用性程度的一项专业评估。

分级评估对产品需求、设计、开发、测试等整个生命周期均有严格的要求，可以为最终用户全面判断产品的安全性好坏提供依据，用户可以结合其对产品的预期使用环境，全方位地衡量该产品是否能够满足自身需

求。同时，评估结果可以帮助用户确定信息安全产品对其预期应用环境而言是否足够安全，以及考量在使用中隐藏的安全风险是否可以被容忍。

历经多年的不间断技术创新和产品研发，“绿盟远程安全评估系统”、“绿盟 WEB 应用防护系统” 已经分别成为这一领域的领导品牌，得到运营商、金融行业、互联网公司、政企等用户的广泛认可，绿盟科技也成为国内惟一一家能够面向全行业用户提供全方位、多层次 WEB 应用漏洞管理解决方案及安全防护的专业厂商，形成了针对 WEB 应用从事前检测、事中防护到事后补偿的端到端解决方案。这两项产品此次获得 EAL3 级证书，进一步稳固了绿盟科技在漏洞扫描类产品市场及 WEB 应用防护产品市场的领导地位。

绿盟科技签署国家信息安全漏洞共享平台协议

10 月 22 日 -23 日，国家计算机网络应急技术处理协调中心 (简称 “国家互联网应急中心”，CNCERT/CC) 主办的 “2009 中国计算机网络安全应急年会” 在长沙举行，绿盟科技应邀出席。会上，国家互联网应急中心、国家信息技术安全研究中心联合绿盟科技等国内近二十家安全公司、软件厂商、互联网企业就共同建设国家信息安全漏洞共享平台的合作事宜举行签约仪式。绿盟科技副总裁吴云坤作为企业代表发言。

吴云坤以分享与协作为主题，强调指出，“漏洞与隐患的消除不是单一产品或是组织可以解决的，需要更大范围的协作。因此，不仅是安全厂商，IT 基础设施提供商、应用开发商等都需要广泛的协作。

软件安全漏洞是构成网络安全威胁的重要原因，网络入侵、大规模蠕虫传播、系统拒绝服务等问题多是由软件安全漏洞所引发。为降低软件安全漏洞带来的风险，增强对漏洞威胁的预警能力，世界上一些发达国家纷纷建立了漏洞集中收集和发布机制。国家互联网应急中心作为国家级网络安全应急组织，多年来为国家互联网基础网络、政府和重要信息系统部门提供网络安全监测、预警和应急处置服务，在应对国家互联网安全突发事件方面发挥了重要作用。

因此，在开放、中立、非盈利性的原则下，国家互联网应急中心、国家信息技术安全研究中心联合国内主流安全公司、软件厂商以及相关互联网企业共建国家信息安全漏洞共享平台 (简称 CNVD)。希望在共建、共享、共赢的理念下，加强国家级网络安全组

织同网络安全企业的合作，共筑国家网络安全防线。

绿盟科技作为漏洞研究的领导者，目前维护着业内最大的中文漏洞信息数据库，收录的漏洞数量近 14000 条，并保持着不间断的更新，及时追踪着最新的安全动向，已经成为国内信息安全漏洞方面事实上的标准和最权威的信息来源，被国内大量媒体引用并使用于安全产品和服务中。同时，绿盟科技有专门的团队负责漏洞信息的收集整理验证工作，已经初步形成了包括漏洞信息采集、验证、录入、更新、发布等环节的完整工作流程，在把漏洞信息运用于产品或服务方面有着丰富的经验。在由资深安全研究专家组成的业界知名的 NSFOCUS 安全小组的支持下，绿盟科技在漏洞技术细节分析和漏洞发掘方面可以提供强大的底层技术支持。凭

借着这些实力，绿盟科技将为国家信息安全漏洞共享平台的建设发挥更大的作用。

绿盟科技致力自主安全，助推“国家漏洞库”建设

中国信息安全测评中心吴世忠主任向获得《信息安全漏洞提交证明》的机构颁发证书

10 月 18 日，中国信息安全测评中心在京宣布我国信息安全“国家漏洞库”正式投入运行。发布会上，以绿盟科技为代表的 20 多家信息安全企业和个人获得了中国“国家漏洞库”信息安全漏洞提交证明。同时会议为首批获得“自主原创证明”的四家国产信息安全产品颁发证书，绿盟网络入侵检测系统 V5.6（NSFOCUS NIDS）获此荣誉。绿盟科技副总裁吴云坤代表公司领奖。

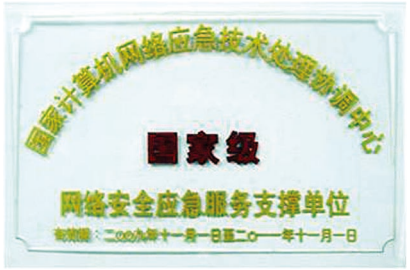
国家漏洞库的建设是信息安全保障工作中一项极为关键的基础性和长期性的工作。当前大量的网络泄密案件和信息安全问题均与漏洞的存在息息相关。中国信息安全测评中心作为我国专门设立的漏洞分析和风险评估职能机构，肩负着国家漏洞库的建设任务。经过半年多的试运行，正式投入运行的“国家漏洞库”已经初具规模，开始为政府部门、产业界及社会提供信息安全漏洞分析和风险评估服务，建立的漏洞收集、分析、通报和面向应用的工作机制，收效明显，这必将极大地提高国家信息安全的威胁应对与风险管理的能力和水平。

同时，中国信息安全测评中心依托“国家漏洞库”的数据资源和软件源代码等方面的独特优势，开展了国产“信息安全产品自主原创证明”的测评业务，在信息安全领域积极落实国家自主创新政策，大力扶持民族信息安全产业的发展，确保国家信息安全实现自主可控的目标。

绿盟科技作为国内安全企业的领导者，一直坚持开发拥有完全自主知识产权的安全产品，为用户提供覆盖脆弱性风险评估和管理、入侵检测和防护、拒绝服务攻击防护、

企业内网终端安全等多个领域的防护能力。公司已经成为拥有自主创新能力的民族信息技术企业，并希望协同各方力量，促进中国信息安全产业在自主原创道路上走得更深更远。

绿盟科技再获 CNCERT/CC 国家级应急服务支撑单位



10 月 11 日，国家计算机网络应急技术处理协调中心 (CNCERT/CC) 应急服务支撑单位评审会在云南腾冲举行。在应急服务规范、应急服务案例、应急服务保证、技术实力、技术优势、与 CNCERT/CC 合作等方面，绿盟科技均获得了评审专家们的一致好评，再次入选国家级应急服务支撑单位。

其中，绿盟科技广州分公司、成都分公司、武汉分公司、西安分公司入选大区级应急服务支撑单位，绿盟科技上海分公司、沈阳分公司、南京办事处、兰州办事处入选省市级应急服务支撑单位。

作为国内最具安全服务经验的公司，绿盟科技在应急服务方面积累了丰富的经验。绿盟科技安全事件响应小组与客户的网络安全中心、应急体系配合协作，共同完成了数百次安全事件的应急响应和处理。完善的专业安全服务体系保障应急响应服务的品质；专业创新的安全产品提供了快速定位、解决安全问题的保证；绿盟科技安全小组、研究部提供知识与技术支持。多年来，绿盟科技为春节联欢晚会、中国东盟博览会、广交会百届盛会、十七大、第 29 届奥运会、温总理与网友在线交流等多项重大活动提供了安全保障。

CNCERT/CC 为了扩展互联网宏观网络安全状况和网络安全事件信息的渠道，增强国家对重大、突发网络安全事件的应对能力，在全国范围内选拔 “CNCERT/CC 网络安全应急服务支撑单位”，绿盟科技凭借优秀的服务能力、众多的应急处理案例、规范的应急处理过程、良好的服务承诺连续多年入选 CNCERT/CC 国家级应急服务支撑单位。

绿盟科技荣膺《财富》杂志卓越雇主榜单

日前，由华信惠悦和《财富》中文版联合评定的 2009 年 “卓越雇主 --- 中国最适宜工作的公司” 榜单揭晓，绿盟科技和腾讯、李宁等 20 家单位荣膺 2009 年度“卓越雇主” 榜单。10 月 14 日，华信惠悦与《财富》杂志在北京万达索菲特大酒店正式举办颁奖典礼，对卓越雇主颁发奖杯。绿盟科技高级副总裁陈文锋出席颁奖典礼。

颁奖典礼上，华信惠悦表示，“绿盟科技在中国拥有高科技行业中最为优秀的人才，公司获此荣誉，我们认为在很大程度上得益于贵公司有着令人向往的工作环境和团队氛围。奖项充分肯定了绿盟科技在人力资源管理上的卓越表现，以及与员工之间所建立起的相互信任、共同发展的共赢关系。”

从 2003 年开始，华信惠悦和《财富》(中文版）就开始合作从事 “卓越雇主” 的研究。每两年一次，迄今为止已经是第四次发布最佳雇主榜单。华信惠悦作为全球著名的人力资源管理咨询公司，本次 “卓越雇主” 排名主要依据华信惠悦 WorkChinaTM 调查计算

出的“雇员敬业度指数”，并根据所有符合标准的公司中被认定为“高敬业员工”的雇员百分比进行排名。评选获奖的标准完全客观和科学，参评企业的“员工效能”得分将作为评选“卓越雇主”的惟一排名标准。

卓越雇主都有着清晰的战略和优秀的领导力，并通过良好的人力资源管理制度营造一个有吸引力的工作环境，打造一支奋进、敬业的团队。绿盟科技自成立以来，一直以“巨人背后的安全专家”为己任，全力为客户服务，本着“诚信为本、客户至上、专业服务、面向国际”的宗旨，汇聚了国内安全领域最优秀的技术研究、产品开发和服务实施队伍。绿盟科技在卓越雇主四项维度的评定中：组织承诺度、战略连接度、工作能力授予度、价值观践行度，公司的得分值都大大超过了市场平均水平。

绿盟科技荣膺 2009 年“卓越雇主”榜单，一方面标志着绿盟科技在人力资源培养、员工敬业度等方面的持续建设获得了国际权威机构的认可；另一方面也将带动公司更优秀的人性化管理体系的建设，进而推动公司持续长远的发展。

绿盟科技石家庄办助力河北国庆安保

在 60 周年国庆到来前夕，绿盟科技石家庄办事处协助河北省信息化办公室对各省直单位和各地市门户网站进行了信息安全大检查，检查发现各网站面临严峻的信息安全风险考验。为了保障国庆期间各网站的安全，9 月 24 日，绿盟科技石家庄办事处协助河北省信息化办公室在石家庄市天桂山培训中心成功举办了“国庆期间河北省网络与信息安全培训班”。

会上，绿盟科技石家庄办技术经理张海波以《政府网站安全防护之道》为主题做了精彩演讲，并在会后和参会人员进行了深入交流。张海波从近期发生的 WEB 安全事件出发，列举了门户网站所面临的安全威胁，并根据这些威胁类型，提出门户网站安全防护之道。同时，还就网站安全渗透报告以及其他安全问题等内容进行了分析。

此次会议针对国庆安保形势，针对性地进行政府网站安保内容的培训，使参会人员

对绿盟科技网站安全防护方案和产品有了更深入的认知，也提升了绿盟科技品牌在河北市场的认知度。

绿盟科技杭州办推进政府网络安全建设

作为政府安保的系列活动，9 月 3 日，绿盟科技杭州办在金华市举办网络安全技术研讨会，进一步探讨如何推进政府网络安全建设。来自政府和事业单位的一些技术人员参加了此次技术交流会。

随着互联网的迅速发展，网络信息安全存在的问题日益加剧，政府行业肩负着整个国家的计划、组织、协调、监控和经济建设的重要职能，除了自身信息安全建设外，对其他行业的客户安全需求也有着重大影响。正是在这样一个背景下，绿盟科技的专家和与会人员分享了近期的政府安全事件与动态、政府部门信息安全工作的建设思路，并就常见的一些安全问题和与会人员进行了互动交流。

会上，绿盟科技的专家大量引用了政府网络安全事件的案例，通过案例分析引出政府部门信息安全建设的工作思路，并就绿盟科技的解决方案做了深入的讲解。通过此次技术交流，进一步提升了绿盟科技在地市级细分区域市场的影响力，也促进了地方政府行业网络安全渠道的建设与推广。

又讯 9 月 15 日，为配合浙江省内各政府机关及教育单位的国庆安保，绿盟科技参加了由浙江省工信委、公安厅、省政府信息中心主办的网络与信息安全研讨会。绿盟科技的技术人员就如何保障政府机关信息网络安全进行了详细的讲解和沟通，并对大家普遍关心的抗 DDoS 攻击进行了深入分析，与会人员也表示出了极大的认同，并表示希望能够进行深入沟通。

绿盟远程安全评估系统 WEB 应用扫描模块全新上市

日前，绿盟科技正式宣布，绿盟远程安全评估系统（原“极光”远程安全评估系统，简称 NSFOCUS RSAS）针对 WEB 应用安全检查的需求，隆重推出专业的 WEB 应用扫描模块。

全新的 NSFOCUS RSAS 产品 WEB 扫描功能，综合应用了很多业内领先的技术，如模拟点击智能爬虫技术、主动挂马检测及核心调度引擎，为用户提供精准的检测结果及最高效的检测效率。可以应用于网站管理员进行 WEB 上线前安全测试、上线后周期性安全评估以及企业安全管理员进行统一的风险监控与管理。

绿盟科技安全专家介绍，相比传统 WEB 扫描器仅局限于提供 WEB 应用层的漏洞扫描，该产品能够为 WEB 应用系统提供最为全面的漏洞检测范围，包含 WEB 应用（SQL 注入漏洞、跨站脚本漏洞、CGI 漏洞，以及网页挂马等漏洞）、WEB 服务及支撑系统（网络层、操作系统层、数据库）等多层次全方位的安全漏洞扫描、审计、渗透测试和辅助逻辑分析。

由于采用专用硬件平台和嵌入式操作系统，以及优化的核心调度引擎，该产品能够提供业内最为高效的检测效率。同时结合多级分布式部署，可以对多个网站群同时并发进行漏洞扫描和风险评估工作，所有扫描结果数据可以由管理节点进行统一的数据汇总、分析和报表呈现。

在操作使用方面，此产品也独具特色，

“一键式”操作模式设计，能够让用户通过最为简单的操作，获得最为专业、全面的评估报告。另外，多用户、多权限划分的用户管理方式，能够由一台设备虚拟成面向多用户独立使用的虚拟设备，从而为用户带来最高性价比的产品，节省用户投资和管理开销。

历经多年的不间断技术创新和产品研发，绿盟远程安全评估系统已经成为这一领域的领导品牌，得到运营商、金融行业、互联网公司、政企以及风险测评机构等用户的广泛认可，绿盟科技也成为国内惟一一家能够面向全行业用户提供多层次漏洞管理解决方案的专业厂商。

绿盟 NIPS 首家获得入侵防护类产品 EAL3 级证书

9 月 16 日，绿盟网络入侵防护系统获得由中国信息安全测评中心颁发的“国家信息安全测评信息技术产品安全测评证书（EAL3 级）”。作为国内入侵防护产品市场的领跑者，绿盟科技是首家也是目前惟一一家获得入侵防护类产品 EAL3 级证书的厂商，代表着 NIPS 技术领域的最高水平。

据悉，信息安全产品分级评估是中国信息安全测评中心依据国家标准 GB/T 18336—2001，综合考虑产品的预期应用环境，通过对信息安全产品的整个生命周期，包括技术、开发、管理、交付等部分进行全面的安全性评估和测试，验证产品的保密性、完整性和可用性程度的一项专业评估。

分级评估对产品需求、设计、开发、测试等整个生命周期均有严格的要求，可以为最终用户全面判断产品的安全性好坏提供依据，用户可以结合其对产品的预期使用环境，全方位地衡量该产品是否能够满足自身需求。同时，评估结果可以帮助用户确定信息安全产品对其预期应用环境而言是否足够安全，以及考量在使用中隐藏的安全风险是否可以被容忍。

绿盟网络入侵防护系统作为首款国内 IPS 产品，一直是绿盟科技的主导产品之一，连续多年获得国内市场各类奖项和荣誉，并在用户群中享有良好口碑。此次产品获得 EAL3 级证书，将进一步促进绿盟 NIPS 产品更好地为安全用户服务。

NSFOCUS 2009年9月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2009-09-08 Microsoft Windows Vista 畸形 SMB 报越界内存引用漏洞

NSFOCUS ID: 13807

http://www.nsfocus.net/vulndb/13807

综述：

Windows 是微软发布的非常流行的操作系统。

Windows Vista 捆绑了新版的 SMB2，SRV2.SYS 驱动没有正确地处理发送给 NEGOTIATEPROTOCOL REQUEST 功能的畸形 SMB 头，如果远程攻击者在发送的 SMB 报文的 Process IdHigh 头字段中包含有 “&” 字符的话，就会在 _Smb2ValidateProviderCallback() 函数中触发越界内存引用，导致执行任意代码或系统蓝屏死机。

危害：

远程攻击者可能利用该漏洞进行拒绝服务攻击甚至执行任意指令。

2. 2009-09-15 Microsoft IIS 脚本文件名错误解析漏洞

NSFOCUS ID: 13830

http://www.nsfocus.net/vulndb/13830

综述：

Microsoft Internet 信息服务（IIS）是 Microsoft Windows 自带的一个网络信息服务器，其中包含 HTTP 服务功能。

IIS 在处理脚本文件名的解析时存在漏洞，当文件名为 [YYY].asp;[ZZZ].jpg 形式时，IIS 会自动以 asp 格式来进行解析，而当文件名为 [YYY].php;[ZZZ].jpg 形式时，IIS 会自动以 php 格式来进行解析（其中 [YYY] 与 [ZZZ] 为可变化字符串）。

危害：

远程攻击者可以利用此漏洞突破 WEB 应用对上传文件类型的限制，在服务器上执行任意脚本代码从而获取对服务器的控制。

3. 2009-09-09 Microsoft DHTML 编辑组件 ActiveX 控件远程代码执行漏洞（MS09-046）

NSFOCUS ID: 13819

http://www.nsfocus.net/vulndb/13819

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 所捆绑的 DHTML 编辑组件 ActiveX 控件（triedit.dll）在格式化 HTML 标记时存在错误。

危害：

攻击者可以通过创建特制网页来利用这个漏洞，如果用户查看

特制的网页，该漏洞可能允许以本地用户的权限执行任意指令。

4. 2009-09-01 Microsoft IIS FTPd 服务 NLST 命令远程栈溢出漏洞

NSFOCUS ID: 13790

http://www.nsfocus.net/vulndb/13790

综述：

Microsoft Internet 信息服务（IIS）是 Microsoft Windows 自带的一个网络信息服务器，其中包含 HTTP 服务功能。

Microsoft IIS 内嵌的 FTP 服务器中存在栈溢出漏洞。如果远程攻击者对带有特制名称的目录发布了包含有通配符的 FTP NLST（NAME LIST）命令的话，就可以触发这个溢出。

危害：

攻击者可以利用此漏洞对服务器进行拒绝服务攻击，如果攻击者可以创建特殊名称的目录则可能成功利用此漏洞控制服务器系统。

5. 2009-09-09 Microsoft Windows TCP/IP 时间戳远程代码执行漏洞（MS09-048）

NSFOCUS ID: 13814

http://www.nsfocus.net/vulndb/13814

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

由于 TCP/IP 栈没有正确地清除状态信息，导致 Windows TCP/IP 栈中存在远程代码执行漏洞。这会导致 TCP/IP 栈引用包含有其他信息的字段为函数指针。

危害：

攻击者可以向在受害者发送特制的 TCP/IP 报文来利用这个漏洞，导致拒绝服务甚至执行任意指令。

6. 2009-09-10 Microsoft Windows TCP/IP 协议栈 0 窗口大小远程拒绝服务漏洞（MS09-048）

NSFOCUS ID: 13823

http://www.nsfocus.net/vulndb/13823

综述：

TCP/IP 是 Internet 最基本的协议、Internet 国际互联网络的基础。

Linux、BSD、Unix、Windows 和 Cisco 产品的 TCP 实现中存在拒绝服务漏洞。通过操控 TCP 连接的状态，攻击者可以强制 TCP 连接处于长期存活（可能为无限期）的状态。如果有足够多的 TCP 连接被强制为长期或无限期存活的状态，就可能耗尽被攻击系统上的资源，导致无法接受新的连接。在某些情况下，必须重启系统才能恢复正常的系统运行。

危害：

攻击者可以利用此漏洞进行拒绝服务攻击。

7. 2009-09-14 Apple Mac OS X 2009-005 更新修复多个安全漏洞

NSFOCUS ID: 13834

http://www.nsfocus.net/vulndb/13834

综述：

Mac OS X 是苹果家族机器所使用的操作系统。

Apple 2009-005 安全更新修复了 Mac OS X 中的多个安全漏洞，其中包括多个缓冲区溢出、内存破坏、整数溢出、跨站脚本等漏洞。

危害：

攻击者可能利用这些漏洞导致拒绝服务、读取敏感信息或执行任意代码。

8. 2009-09-10 Firefox 3.5.3/3.0.14 版本修复多个安全漏洞

NSFOCUS ID: 13822

http://www.nsfocus.net/vulndb/13822

综述：

Firefox 是 Mozilla 所发布的开源 WEB 浏览器。

Firefox 修复了多个安全漏洞，包括内存破坏，权限提升、执行安全操作可能被绕过等漏洞。

危害：

攻击者可以利用这些漏洞导致拒绝服务、欺骗攻击甚至入侵用户系统。

9. 2009-09-07 动网论坛 DvBBS boardrule.php 模块 SQL 注入漏洞

NSFOCUS ID: 13804

http://www.nsfocus.net/vulndb/13804

综述：

DVBBS 是一款 Aspsky.Net 开发和维护的开放源码 ASP WEB 论坛程序。DvBBS 没有正确地过滤用户提交给 boardrule.php 模块的 groupboardid 参数，远程攻击者可以通过向论坛提交恶意参数请求执行 SQL 注入攻击。

危害：

攻击者可以利用此漏洞获取或篡改论坛系统的敏感数据。

10. 2009-09-04 PPStream MList.ocx ActiveX 控件多个缓冲区溢出漏洞

NSFOCUS ID: 13801

http://www.nsfocus.net/vulndb/13801

综述：

PPS 网络电视（PPStream）是全球第一家集 P2P 直播点播于一身的网络电视软件。

PPStream 所提供的 PPSMediaList 控件（MList.ocx）没有正确地验证多个输入参数，如果用户受骗访问了恶意网页并向该控件传送了超长参数，就可以触发多个缓冲区溢出。

危害：

攻击者可以通过创建特制网页来利用这个漏洞，如果用户查看特制的网页，该漏洞可能允许以本地用户的权限执行任意指令。

NSFOCUS 2009年10月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) **安全小组** <security@nsfocus.com> **根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。**http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2009-10-14 Microsoft Windows SMB2 命令值远程代码执行漏洞（MS09-050）

NSFOCUS ID: 13924

http://www.nsfocus.net/vulndb/13924

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 系统的 SMB 实现在处理 SMB 多协议协商请求报文时没有使用经过验证的命令值拷贝，未经认证的远程攻击者可以通过向运行 Server 服务的计算机发送特制的 SMBv2 报文来利用这个漏洞。

危害：

攻击者可以利用此漏洞控制受害者系统。

2. 2009-10-20 Microsoft GDI+ 库图形文件处理多个缓冲区溢出和内存破坏漏洞 (MS09-062)

NSFOCUS ID: 13942

http://www.nsfocus.net/vulndb/13942

综述：

Microsoft 产品中所使用的 GDI+ 库（GdiPlus.dll）通过基于类的 API 提供对各种图形方式的访问。

GDI+ 处理畸形 WMF、PNG、TIFF、BMP 等图形文件时存在多个缓冲区溢出和内存破坏漏洞。这些漏洞影响包括 Office 和 Internet Explorer 等多个软件。

危害：

攻击者可以诱使受害者察看包含恶意图片的网页或 Office 文档，从而控制受害者系统。

3. 2009-10-15 Microsoft IE deflate HTTP 内容编码远程代码执行漏洞（MS09-054）

NSFOCUS ID: 13936

http://www.nsfocus.net/vulndb/13936

综述：

Internet Explorer 是 Windows 操作系统中默认捆绑的 WEB 浏览器。

Internet Explorer 的 Content-Encoding:deflate 实现中存在内存破坏漏洞，在特定情况下处理数据流头可以触发这个漏洞。

危害：

攻击者可以诱使受害者察看特制的网页，从而控制受害者系统。

4. 2009-10-15 Microsoft IE HTML 组件处理远程代码执行漏洞（MS09-054）

NSFOCUS ID: 13935

http://www.nsfocus.net/vulndb/13935

综述：

Internet Explorer 是 Windows 操作系统中默认捆绑的 WEB 浏览器。

Internet Explorer 在特定情况下处理变量的参数验证的方式中存在漏洞。

危害：

攻击者可以诱使受害者察看特制的网页，从而控制受害者系统。

5. 2009-10-14 Microsoft Windows Media Player ASF 文件解析堆溢出漏洞（MS09-052）

NSFOCUS ID: 13928

http://www.nsfocus.net/vulndb/13928

综述：

Windows Media Player 是微软操作系统中默认捆绑的媒体播放器。

Windows Media Player 6.4 在处理特制的 ASF 文件时存在堆溢出漏洞。

危害：

攻击者可以诱使受害者察看特制的 ASF 文件，从而控制受害者系统。

6. 2009-10-16 Microsoft Windows 索引服务 ActiveX 控件内存破坏漏洞（MS09-057）

NSFOCUS ID: 13937

http://www.nsfocus.net/vulndb/13937

综述：

Windows 是微软发布的非常流行的操作系统。

Windows 的索引服务所包含的 ActiveX 控件未正确处理特制 WEB 内容，导致 Windows 系统上的索引服务中存在内存破坏漏洞。

危害：

攻击者可以诱使受害者察看特制的网页，从而控制受害者系统。

7. 2009-10-16 Microsoft Windows 内核本地权限提升和拒绝服务漏洞（MS09-058）

NSFOCUS ID: 13938

http://www.nsfocus.net/vulndb/13938

综述：

Windows 是微软发布的非常流行的操作系统。

由于错误地将 64 位至截断为 32 位值，以及未充分验证用户态

传递的某些数据，导致 Windows 内核中存在权限提升漏洞。

危害：

成功利用此漏洞的攻击者可以运行任意内核态代码。此外由于内核处理特定异常方式而导致 Windows 内核中存在拒绝服务漏洞。

8. 2009-10-20 UiPlayer UiCheck 组件栈溢出漏洞

NSFOCUS ID: 13943

http://www.nsfocus.net/vulndb/13943

综述：

UiPlayer 网络视频播放软件是联合网视（UITV）公司的视频播放软件。

UiPlayer 的安装目录下的 UiCheck.dll 是一个 ActiveX 控件，UiCheck.dll 提供了一个接口函数 GetUiDllVersion()，该函数会把接收到的文件名参数拷贝到一个固定大小的缓冲区，如果文件名超长，就会导致栈溢出。因为和百度等公司的合作，很多视频播放软件中也集成 了 UiPlayer，例如百度下吧等。

危害：

攻击者可以诱使受害者察看特制的网页，从而控制受害者系统。

9. 2009-10-19 Adobe APSB09-15 更新修复多个安全漏洞

NSFOCUS ID: 13941

http://www.nsfocus.net/vulndb/13941

综述：

Adobe Acrobat/Adobe Reader 是非常流行的 PDF 文件阅读器。

APSB09-15 更新修复了 Adobe Reader 和 Acrobat 中的多个安全漏洞，其中包括多个堆溢出、整数溢出、内存破坏、认证绕过和跨占脚本等问题。用户受骗打开畸形的 PDF 文档就会导致拒绝服务、绕过安全限制或完全入侵用户系统。

危害：

攻击者可以诱使受害者察看特制的 pdf 文档，从而控制受害者系统。

10. 2009-10-09 IBM AIX rpc.cmsd 守护进程栈溢出漏洞

NSFOCUS ID: 13903

http://www.nsfocus.net/vulndb/13903

综述：

IBM AIX 是一款商业性质的 UNIX 操作系统。

AIX 的日历守护进程库 libcsa.a 中存在栈溢出漏洞。rpc.cmsd 日历守护进程在处理对 21 号远程过程的请求时函数取了两个 XDR 字符串参数并将第一个拷贝到了栈缓冲区。由于缺少长度检查，这个拷贝操作可能溢出。

危害：

攻击者可以利用此漏洞控制服务器系统。

NSFOCUS 2009年11月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2009-11-11 Microsoft Windows License Logging 服务远程堆溢出漏洞（MS09-064）

NSFOCUS ID: 14057

http://www.nsfocus.net/vulndb/14057

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 系统中的 License Logging 服务（llssrv.exe）处理 RPC 调用的方式堆溢出漏洞。在处理传送给 LlsrLicenseRequestW 方式的参数时，字符数组应包含有终止的空字符。如果用户发送了没有空字符的恶意请求数据，就可以覆盖对 lstrcatW 的调用，触发这个溢出。利用这个漏洞无需认证。

危害：

攻击者可以通过向运行 License Logging 服务的计算机发送特制网络消息来利用这个漏洞，成功利用这个漏洞允许攻击者完全控制系统。

2. 2009-11-10 Microsoft Windows 嵌入式 OpenType 字体引擎远程代码执行漏洞 (MS09-065)

NSFOCUS ID: 13785

http://www.nsfocus.net/vulndb/13785

综述：

Microsoft Windows 是微软开发的非常流行的操作系统。

Windows Server 2003 SP2 的嵌入式 OpenType（EOT）字体引擎所使用的 win32k.sys 驱动在构建目录项时没有正确的解析字体代码。如果用户受骗打开的 HTML 文档中 @font-faceCSS 规则的 src 描述符引用了特制的 .eot 文件, 就可能导致执行任意内核态代码。

危害：

攻击者可以诱使受害者浏览嵌入了恶意 .eot 文件的网页来利用这个漏洞，成功利用这个漏洞允许攻击者完全控制系统。

3. 2009-11-09 多个厂商 TLS 协议会话重新协商中间人攻击漏洞

NSFOCUS ID: 14046

http://www.nsfocus.net/vulndb/14046

综述：

传输层安全协议（TLS）是确保互联网上通信应用和其用户隐私的协议。

多个厂商的 TLS 协议实现中的会话重新协商过程受中间人攻击的影响，扮演为中间人的恶意服务器可以向应用协议流的开始处注入受控的明文，这有助于各种网络欺骗攻击。

危害：

攻击者可以利用这个漏洞进行钓鱼攻击。

4. 2009-11-12 Microsoft Excel索引解析内存破坏漏洞(MS09-067)

NSFOCUS ID: 14068

http://www.nsfocus.net/vulndb/14068

综述：

Excel 是微软 Office 套件中的电子表格工具。

Excel 解析单元格中嵌入了特制公式的文档时存在内存破坏漏洞。

危害：

攻击者可以诱使受害者打开嵌入恶意公式的 Excel 文档来触发此漏洞，成功利用这个漏洞允许攻击者完全控制系统。

5. 2009-11-11 Microsoft Windows WSDAPI 服务远程内存破坏漏洞（MS09-063）

NSFOCUS ID: 14058

http://www.nsfocus.net/vulndb/14058

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

Windows 系统中设备 API 上 WEB 服务（WSDAPI）中存在内存破坏漏洞。

危害：

远程攻击者可以通过向 WSDAPI 服务发送带有畸形头的 WSD 消息触发这个漏洞，成功利用这个漏洞允许攻击者完全控制系统。

6. 2009-11-11 Microsoft Word 记录解析栈溢出漏洞(MS09-068)

NSFOCUS ID: 14054

http://www.nsfocus.net/vulndb/14054

综述：

Word 是微软 Office 套件中的文件处理工具。

Word 处理包含有畸形文件信息块（FIB）结构的特制 Word 文件的方式中存在栈溢出。

危害：

攻击者可以诱使受害者打开嵌入恶意 FIB 结构的 Word 文档来触发此漏洞，成功利用这个漏洞允许攻击者完全控制系统。

7. 2009-11-06 Oracle 数据库 Resource Manager 组件远程溢出漏洞

NSFOCUS ID: 14041

http://www.nsfocus.net/vulndb/14041

综述：

Oracle Database 是一款商业性质大型数据库系统。

Oracle 数据库 Resource Manager 组件的 ALTER SYSTEM SET RESOURCE_MANAGER_PLAN 语句和 SYS.DBMS_RESOURCE_MANAGER.SWITCH_PLAN 过程中存在缓冲区溢出漏洞。

危害：

拥有 ALTER SYSTEM 权限的用户可以通过提交超长的 plan name 字符串来触发这个溢出，导致 Oracle 服务进程崩溃或执行任意代码。

8. 2009-11-05 Adobe Shockwave Player 多个远程代码执行和拒绝服务漏洞

NSFOCUS ID: 14029

http://www.nsfocus.net/vulndb/14029

综述：

Adobe Shockwave Player 是专门播放使用 Director Shockwave Studio 制作的网页的外挂软件。

Shockwave Player 中存在多个无效索引、无效指针和堆溢出漏洞。

危害：

攻击者可以诱使受害者打开恶意网页来触发此漏洞，成功利用这个漏洞允许攻击者完全控制系统。

9. 2009-11-03 Firefox 多个内存破坏漏洞

NSFOCUS ID: 14015

http://www.nsfocus.net/vulndb/14015

综述：

Firefox 是一款流行的开源 WEB 浏览器。

Firefox 所使用的 liboggz、libvorbis 和 liboggplay 媒体渲染库及浏览器引擎、JavaScript 引擎中存在多个内存破坏漏洞。

危害：

攻击者可以诱使受害者打开恶意网页或媒体文件链接来触发此漏洞，成功利用这个漏洞允许攻击者完全控制系统。

10. 2009-11-06 Sun Java JDK/JRE 安全更新修复多个漏洞

NSFOCUS ID: 14035

http://www.nsfocus.net/vulndb/14035

综述：

Solaris 系统的 Java 运行时环境（JRE）为 JAVA 应用程序提供可靠的运行环境。

Sun Java 的 2009 年 11 月份更新修复了多个安全漏洞，其中包括多个栈溢出、整数溢出、内存耗尽和认证绕过问题。

危害：

远程攻击者可以利用这些漏洞绕过安全限制、导致拒绝服务或完全入侵用户系统。

NSFOCUS 2009年12月之十大安全漏洞

声明：本十大安全漏洞由 NSFOCUS(绿盟科技) 安全小组 <security@nsfocus.com> 根据安全漏洞的严重程度、利用难易程度、影响范围等因素综合评出，仅供参考。http://www.nsfocus.net/index.php?act=sec_bug&do=top_ten

1. 2009-12-01 FreeBSD execl() 函数本地权限提升漏洞

NSFOCUS ID: 14152

http://www.nsfocus.net/vulndb/14152

综述：

FreeBSD 就是一种运行在 Intel 平台上、可以自由使用的开放源码 Unix 类系统。

正常情况下 FreeBSD 的运行时链接编辑器（rtld）不允许在执行 ping 或 su 等 setugid 二进制程序时设置类似于 LD_PRELOAD 的危险环境变量，但本地用户可以通过 execl() 函数诱骗 rtld 接受 setugid 二进制程序的 LD 变量, 导致以 root 用户权限执行任意代码。

危害：

攻击者可以利用此漏洞提升权限，对系统资源进行非授权的访问。

2. 2009-12-02 多个厂商无客户端 SSL VPN 产品绕过同源策略漏洞

NSFOCUS ID: 14157

http://www.nsfocus.net/vulndb/14157

综述：

无客户端 SSL VPN 允许用户无需安装传统的 VPN 客户端就可以基于浏览器访问内部和外部资源。

如果攻击者所创建的网页可以混淆 document.cookie 元素以防被 WEB VPN 重写，则返回页面中的 document.cookie 对象就会代表 WEB VPN 域所有的用户 Cookie。

危害：

攻击者可以利用这些 Cookie 劫持用户的 VPN 会话和依赖于 Cookie 识别会话的 WEB VPN 所访问的所有其他会话。

3. 2009-12-09 Microsoft IE XHTML DOM 操控内存破坏漏洞（MS09-072）

NSFOCUS ID: 14189

http://www.nsfocus.net/vulndb/14189

综述：

Internet Explorer 是 Windows 操作系统中默认捆绑的 WEB 浏览器。

Internet Explorer 操控和解析某些 HTML 标签的方式存在内存破坏漏洞，以畸形方式获得各种对象会导致调用悬浮指针，这可以通过 heapspray 进一步利用。

危害：

攻击者可以通过构建特制的网页来利用该漏洞，当用户查看网页时，该漏洞可能允许远程执行代码。

4. 2009-12-09 Microsoft Windows IAS 服务远程内存破坏漏洞（MS09-071）

NSFOCUS ID: 14194

http://www.nsfocus.net/vulndb/14194

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

由于在处理受保护可扩展认证协议（PEAP）认证尝试时内存中错误的拷贝了服务器所接收到的消息，导致 Internet 认证服务的 PEAP 实现中存在内存破坏漏洞。

危害：

攻击者可以向服务器发送恶意数据来利用该漏洞，从而控制服务器系统。

5. 2009-12-09 Microsoft ADFS 服务请求头验证远程代码执行漏洞（MS09-070）

NSFOCUS ID: 14187

http://www.nsfocus.net/vulndb/14187

综述：

Microsoft Windows 是微软发布的非常流行的操作系统。

由于通过认证的用户在连接到启用了活动目录联合服务（ADFS）的 WEB 服务器时没有正确地验证请求头，导致 ADFS 实现中存在远程代码执行漏洞。

危害：

远程攻击者可以通过向服务器提交恶意的 HTTP 请求导致以 Worker ProcessIdentity 的权限执行任意代码。

6. 2009-12-10 Adobe Flash Player JPEG 解析堆溢出漏洞

NSFOCUS ID: 14200

http://www.nsfocus.net/vulndb/14200

综述：

Flash Player 是一款非常流行的 FLASH 播放器。

Flash Player 在解析 SWF 文件中所包含的 JPEG 维度时计算图形的帧大小缺少过滤检查，用户受骗打开恶意的 JPEG 图形就可以触发堆溢出。

危害：

攻击者可以诱使受害者打开恶意的 SWF 文件，从而控制受害者系统。

7. 2009-12-09 Microsoft 写字板和 Office 文本转换器 Word 97 文件解析远程代码执行漏洞（MS09-073）

NSFOCUS ID: 14197

http://www.nsfocus.net/vulndb/14197

综述：

写字板是Windows操作系统中附件所提供的简单文本编辑工具。

当用户打开特制的 Word 97 文件时，Microsoft 写字板和 Word 文本转换器中的内存破坏漏洞可能导致执行任意代码。

危害：

攻击者可以诱使受害者打开恶意的 Word 97 文件，从而控制受害者系统。

8. 2009-12-10 HP OpenView 网络节点管理器多个缓冲区溢出和命令注入漏洞

NSFOCUS ID: 14201

http://www.nsfocus.net/vulndb/14201

综述：

HP OpenView 网络节点管理器（OV NNM）是 HP 公司开发和维护的网络管理系统软件，具有强大的网络节点管理功能。

OV NNM 的 ovWEBsnmpsrv.exe、snmpviewer.exe、ovalarm.exe、WEBappmon.exe、ovsessionmgr.exe、nnmRptConfig.exe、snmp.exe 等进程存在多个栈溢出和堆溢出漏

危害：

攻击者可以向 OV NNM 的服务进程提供超长数据来触发这些漏洞，从而控制服务器系统。

9. 2009-12-07 Linux Kernel HFS 子系统栈溢出漏洞

洞

NSFOCUS ID: 14176

http://www.nsfocus.net/vulndb/14176

综述：

Linux Kernel 是开放源码操作系统 Linux 所使用的内核。

Linux Kernel 的 fs/hfs/dir.c 文件中的 hfs_readdir 函数存在栈溢出漏洞，特制的多级文件系统（HFS）可以在 hfs_bnode_read() 函数的 memcpy() 调用过程中触发这个溢出。

危害：

攻击者可以诱使受害者打开恶意的媒体文件，从而控制受害者系统。

10. 2009-12-18 Winamp 模块解码器插件多个堆溢出漏洞

NSFOCUS ID: 14233

http://www.nsfocus.net/vulndb/14233

综述：

Winamp 是一款流行的媒体播放器，支持多种文件格式。

Winamp 的模块解码器插件（IN_MOD.DLL）在解析 Impulse Tracker 文件中乐器定义、样例和 Ultratracker、Oktalyzer 文件时存在多个堆溢出漏洞。

危害：

攻击者可以诱使受害者打开特制的媒体文件，从而控制受害者系统。

巨人背后的专家

- 2009年：荣获Frost&Sullivan颁发的“2009年中国IDS/IPS市场增长战略领导者”奖
- 2008年：绿盟科技“极光”远程安全评估系统成为1996年以来全球大家获得英国西海岸实验室权威认证的漏洞扫描产品之一
- 2007年：再次入选国家级应急服务支撑单位
- 2006年：连续四年荣获中计报“值得信赖的安全服务品牌”
- 2005年：囊括年度入侵检测\保护系统全部奖项
- 2004年：入选公共互联网应急处理国家级服务试点单位
  首批荣获国家二级安全服务资质
- 2003年：进入中国电子政务IT百强
- 2002年：承担全国性电信网安全评估
- 2001年：入选国家网络安全服务试点单位
- 2000年：绿盟科技成立

www.nsfocus.com

THE EXPERT
BEHIND GIANTS

长期以来，绿盟科技致力于网络安全技术的研究，为军工、政府、电信、金融、能源等行业提供优质的安全产品与服务。在这些巨人的背后，他们是值受信赖的专家。

NSFOCUS

THE EXPERT BEHIND GIANTS 巨人背后的专家

Nsmagazine@nsfocus.com