Neusoft

安全加固服务白皮书

沈阳东软系统集成工程有限公司

2012 年 3 月

文档名称	NSS-WP-02-安全加固服务白皮书
基本说明	介绍东软安全服务团队提供的安全加固服务。
文档编号	NSS-WP-02
扩散范围	对安全加固服务有需求的组织。

地　　址：北京市海淀区东北旺西路 8 号中关村软件园 6 号楼

邮　　编：100029

电　　话：(86 10) 5651 7887

传　　真：(86 10)8282 6052

目 录

1 安全加固服务概述

随着互联网应用的纵深演进，网络安全的概念已经不仅仅限于单一的安全产品和技术，而是涉及到企业和组织范围内网络体系各个层面的动态防护与安全管理。为了让客户能够充分了解到自身内部的安全威胁和风险，以便能够进行完善的安全体系保障建设，东软利用自己的安全技术和丰富的经验，为客户提供专业的安全评估服务。

安全加固则更强调针对主机和系统的安全保护加强，安全加固通常建立在安全风险评估的结果基础之上，参照安全评估结果的《安全风险评估报告》和《安全解决方案》，对评估对象进行安全加固。

1.1安全加固的目的

安全加固工作的目标是解决在安全评估中发现的技术性安全问题，所有的被评估对象应不再存在高风险漏洞和中风险漏洞（根据 CVE 标准定义）。同时，在此过程中注意避免影响修补加固对象原有的功能和性能（若可能存在，必须事先指出，并进行周密的计划和布置规避相应的风险）。

安全加固首先要让加固对象满足安全基线要求，这是安全加固的基本目标。并采用优化配置、调整安全策略、安装补丁、安装安全软件等方式进行，在尽量不影响修补加固对象原有功能和性能的基础上，解决在安全评估中发现的安全问题，修补其中存在的漏洞。

安全加固也不仅仅局限于单独的加固对象，对象所处的环境，包括其他安全设备的安全防护（比如入侵检测系统、防火墙等）、网络结构等，都属于需要考虑的范围。在加固实施中，东软也将这些部分对加固对象的保护中提出积极、可靠的建议。

安全加固也是组织所制定的安全策略的实施实践，从实践的角度来检验安全策略的有效性。

因此，安全加固的目的是：

1. 确保对象满足安全基线要求；

2. 优化配置，安装适用的安全软件等加强对象的安全性能；

3. 从实践角度检验安全策略的有效性。

在安全加固过程中遵循严格的风险控制策略，避免对系统造成破坏和影响。

1.2安全加固的必要性

从安全加固的目的，可以看出，安全加固是一项对主机系统等进行的基本安全保护措施，通过安全加固一方面能够修补系统中的安全漏洞，同时也优化了配置，加强了对象的安全性。这对于安全保护来说，是非常必要的。

安全加固并非一项单纯的技术性操作，它也将同时反映出组织所制定的安全策略的有效性。比如针对某个主机进行的安全加固，将涉及到多方面的安全策略：账号密码的制定策略、账号密码的管理策略、访问控制策略、审计审核策略等，并且也会密切联系一些安全设备，比如防火墙、交换机等的安全保护控制。

1.3安全加固的原则

东软安全加固服务遵循以下原则：

1. **标准性原则**

加固方案的设计与实施应依据国内或国际的相关标准进行。标准性原则确保安全加固过程的规范、合理，并为安全加固成果提供了质量保证。

2. **规范性原则**

服务提供商提供规范的工作中的过程和文档，具有很好的规范性，可用于项目的跟踪和控制。安全加固项目形成如下文档：

- 项目计划——针对具体的今后一段时间的安全加固项目进展，制订具体的项目计划。
- 工作确认单——针对每天的安全加固工作，形成工作确认单进行备案。
- 阶段工作完成单——针对阶段性的工作进展，形成阶段工作确认单。
- 安全加固服务报告——安全加固服务完成后提供安全加固服务过程的书面报告，包括安全加固服务过程，记录所有操作和相应的目的以及加固后的安全水平的提升说明。
- 灾难恢复计划——在安全加固服务完成期限内提供的书面安全事件响应计划，包括安全故障或灾难发生时，相关维护人员应采取的操作流程，东软可提供的紧急响应服务流程等。

3. 加固优先级原则

加固操作应优先解决高危风险漏洞，其次解决中风险漏洞、低风险漏洞。

4. 可控性原则

加固的方法和过程要在客户认可的范围之内，加固服务的实际进度与进度表安排一致，保证客户对于加固工作的可控性。

5. 整体性原则

加固的范围和内容应当整体全面，包括安全涉及的各个层面，以免由于遗漏造成未来的安全隐患。

6. 最小影响原则

加固工作应尽可能小的影响系统和网络的正常运行，不能对正在的运行和业务的正常提供产生显著不利影响。具体体现在项目实施的时候，首先，安全加固在业务不繁忙时段进行；其次，有主备的主机系统和设备，首先在备机上进行安全加固，确信对业务系统不会有不利影响后方在主机上实施相应的安全加固；对于特别重要的系统和设备，若不满足直接对本机进行安全加固的条件，则应考虑采取其他更为稳妥的安全措施（如：考虑在其边界部署安全防护措施）。

7. 保密原则

东软对加固的过程数据和结果数据严格保密，确保所有的阅读和使用均经过客户的授权，项目关闭后所有客户提供资料和与客户信息资产相关的资料均安全删除。

2 安全加固服务内容

为帮助客户加强系统的安全性能，并且能够让客户自定义需要的加固内容，东软将安全加固服务划分为细小的服务组件，这些服务组件可以单独进行，并提供给客户进行个性化选择，东软也可以为客户提供咨询建议，以便客户能够更方便获得需要的服务。

安全加固服务包含表所示组件：

组件名称	主要内容
操作系统加固	通过全面了解服务器操作系统运行状况和安全状况，采取补丁修补，并优化和加强账号口令、日志审核、网络性能、文件系统、权限控制、服务和进程等的安全性能。包括各种操作系统：Windows、Linux、各种 Unix 等
数据库加固	通过了解数据库系统的运行状况，采取补丁修补，并优化和加强账号口令、日志审核、网络属性、相关文件、数据库配置（存储过程）等的安全性能。包括各种数据库系统：SQL Server、MySQL、DB2、Sybase、Informix 等
应用服务加固	通过了解常见应用服务的运行状况和安全状况，采取补丁修补，并优化和加强应用属性、日志审核、目录和相关文件等的安全性能。包括常见的各种应用：Web、Mail、DNS 等
网络设备与安全设备加固	通过了解各种网络、安全设备的运行状况和安全状况，采取升级，并优化和加强访问控制、账号口令、网络属性、服务等的安全性能。这些网络、安全设备包括各个厂商的路由器、交换机、防火墙等

3 安全加固的时间

安全加固的实施过程同加固对象的数量有着密切的联系。同时，东软建议在实施过程中客户应该安排人员陪同；因此，也将同客户人员的工作安排相关联。

但是，一般的实施过程（不包括评估过程，5~7 个加固对象）通常需要 7 到 8 个工作日，时间安排大致为：

- 制定方案与申请确认 2 到 3 个工作日
- 加固实施在 2 到 3 个工作日内
- 检查评估在 2 个工作日内
- 报告撰写时间为 1 到 2 个工作日。

4 东软安全加固服务流程

东软认为，一个典型的安全加固服务过程，通常可以分为下面五个阶段：制定方案、申请与确认、操作实施、检查评估、产生报告。

图 4-1 是一个普遍的安全加固服务实施的流程：

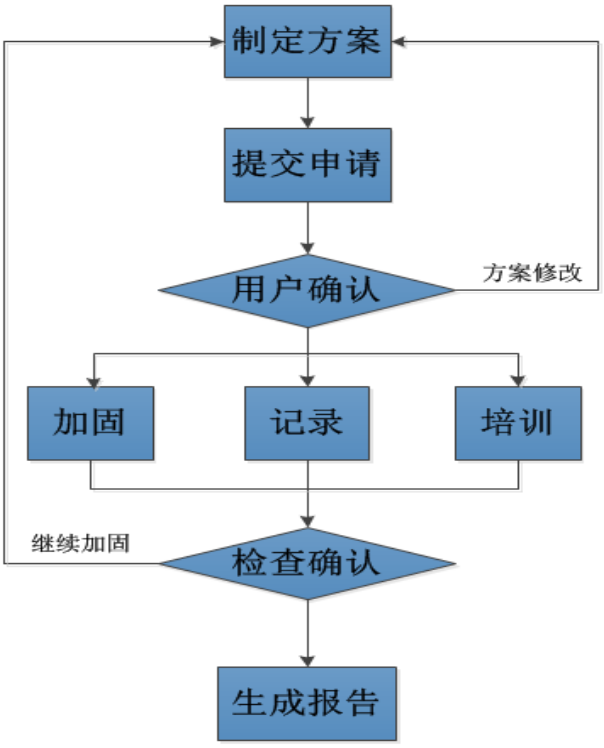

图 4-1: 安全加固服务实施流程

4.1 制定方案

制定方案阶段主要是根据前期的安全评估结果，分析评估结果中的系统存在的风险，制定《安全加固方案》，安全加固方案是操作实施的指导性文档，同时也包含风险规避措施等内容。

4.2 申请与确认

方案制定之后，将向客户提交加固申请。如果客户对方案中的操作存在疑问或者提出的修改建议，那么将根据情况，对《安全加固方案》进行相应的调整和修改。

经过客户的确认后，才将进行加固的操作实施。

4.3 操作实施

操作实施阶段就是主要的技术性加固实施。本阶段将依据加固方案对加固对象进行操作，可能包括补丁修补、账号密码加强、访问控制加强、网络属性加固、日志审核加强、常见网络服务加强等。

对于安全补丁的安装，由于一些厂商发布的安全补丁稳定性不高，可能造成系统异常，因此，建议在加固操作实施前先进行系统备份，以便在出现异常后能够快速恢复。

在操作过程中，东软的安全工程师将同时将各个操作进行纪录，这种规范操作将能帮助客户了解操作内容和所做修改，并且，东软的安全工程师也会同客户相关技术人员进行密切的沟通，并进行安全加固的现场培训，让客户的技术人员能够了解加固内容和相关操作。

安全加固过程中将对系统进行配置的修改或者补丁的安装，以达到安全加强的目的；虽然，在安全加固的过程中会存在一些安全风险，比如一些操作系统开发商提供的安全补丁会影响现有系统本身的稳定性等；但是，当安全加固

操作出现异常后，东软的安全工程师将协同客户相关技术人员，根据前期已经制定的安全规避方案进行修复，以将风险控制在最小范围内，并产生《故障恢复报告》。

4.4 检查评估

检查评估阶段主要是客户（或第三方）或者东软对安全加固实施后的系统进行重新的安全评估，检查安全加固操作是否被正确实施，同时也检查安全加固是否有效。

检查评估是必要的，这将帮助客户检查实施工作，并确保操作实施的正确性和有效性。

4.5 产生报告

产生报告阶段将根据前面各个阶段的工作内容，形成《安全加固报告》。

5 东软安全加固服务特点

安全加固是一项对经验与技术要求都很高的技术操作项目，在不具备充分能力（对系统的熟悉和对入侵手段的了解）的情况下，简单的配置操作不能确保系统的安全性。

东软通过多年的专业技术积累以及对黑客技术的研究和跟踪，能够针对网络系统中的 Windows、Unix、Linux 等各类操作系统的服务器、数据库服务器、各类品牌的网络通讯设备，包括可管理的交换机、路由器，以及各类标准服务类软件，进行安全加固。

东软有自己的安全加固操作流程和规范。在很多安全操作方面，东软的安全专家将密切与客户交流和沟通。通过东软的安全加固服务，能够让客户的系统更安全。

东软是一家拥有雄厚安全服务能力的网络安全公司，可以保证为客户提供国内先进、乃至国际一流的安全加固评估服务。

- **工程经验：**东软已经对多个电信、国家机关、公安、军队、新闻机构乃至国外客户成功的提供过安全加固服务，具有丰富的工程实施经验。

- **技术积累：**东软有自己的积极防御实验室，是国内最具实力的网络安全研发队伍之一，对渗透测试服务提供的强大的人员、技术支持。

- **服务资质：**东软拥有业界最强的信息安全服务能力资质，计算机信息系统集成一级资质（唯一）、涉密信息系统集成甲级资质（最高级）、国家信息安全服务二级资质（最高级）、信息安全风险评估服务一级资质（最高级）、国家级应急响应技术支撑单位（最高级）、国家注册信息安全人员 CISP 授权培训机构、CIW 中国唯一战略合作伙伴、ISO 9001 信息技术服务质量体系认证、ISO 27001 信息安全管理体系认证、CMMI5 系统工程能力成熟度认证（最高级）、2008 北京奥运安保技术支撑单位、2010 广州亚运会及上海世博会、2011 大运会网络安全保障支持单位。

- **信息控制：**东软具有国家保密局颁发的涉密信息系统集成甲级资质（最高级）。具有各种重要单位，甚至涉密单位提供服务的能力和资质。在公司内部员工和客户信息有着严格的信息控制手段，保证客户的敏感信息的安全性。