Neusoft

应急响应服务白皮书

沈阳东软系统集成工程有限公司

2012 年 3 月

文档说明

文档名称	NSS-WP-07-应急响应服务白皮书
基本说明	介绍东软安全服务团队提供的应急响应服务。
文档编号	NSS-WP-07
扩散范围	对应急响应服务有需求的组织。

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 东软应急响应服务介绍

在组织运营维护自己的业务系统过程中，系统管理员由于时间和精力的问题，常常对于一些紧急安全事件缺乏有效的处理，这样往往会对业务系统的正常、连续运转造成重大影响。面对现今复杂的网络安全环境，越来越多的企事业单位开始考虑将信息安全事件的应急响应进行服务外包，从而可以更好的降低重大信息安全事件的影响面。

作为国内领先的整体信息安全解决方案提供商，东软拥有专业的信息安全服务团队 NCSIRT（Neusoft Computer Security Incident Response Team），以及投资 4000 万元组建的信息安全攻防研究实验室和解决方案验证中心，同时东软也是中国最大的漏洞库提供者之一。2004 年，东软入选首批国家计算机网络应急技术处理协调中心“公共互联网应急处理国家级服务试点单位”，2007 年成为首批正式国家级应急服务支撑单位。近 10 年来为各行业客户组织处理了包括大规模病毒爆发、网络入侵事件、拒绝服务攻击、主机或网络异常事件在内的上百项重大紧急事故，以最快速度恢复系统的保密性、完整性和可用性，保障客户组织业务系统的连续性，阻止和减小安全事件带来的负面影响。

2 东软应急响应服务形式

1. 本地应急响应

- 由项目管理组指派安全服务工程师在第一时间赶往客户现场进行处理。原则上，对本地范围内的用户，3—6 小时到达现场；对异地用户，24 小时内到达现场。

2. 远程应急响应（备选，仅当事件并非应急时）

- 用户通过电话、Email、传真等方式请求安全事件响应，应急响应组通过相同的方式为用户解决问题。
- 当无法通过远程访问的方式为用户解决问题时，经用户确认后，转到本地应急响应相关流程，同时此次远程响应无效，归于本地应急响应类型。

3 东软应急响应服务流程

东软的应急响应流程主要分为三个阶段：

第一阶段： 事件预警与通知

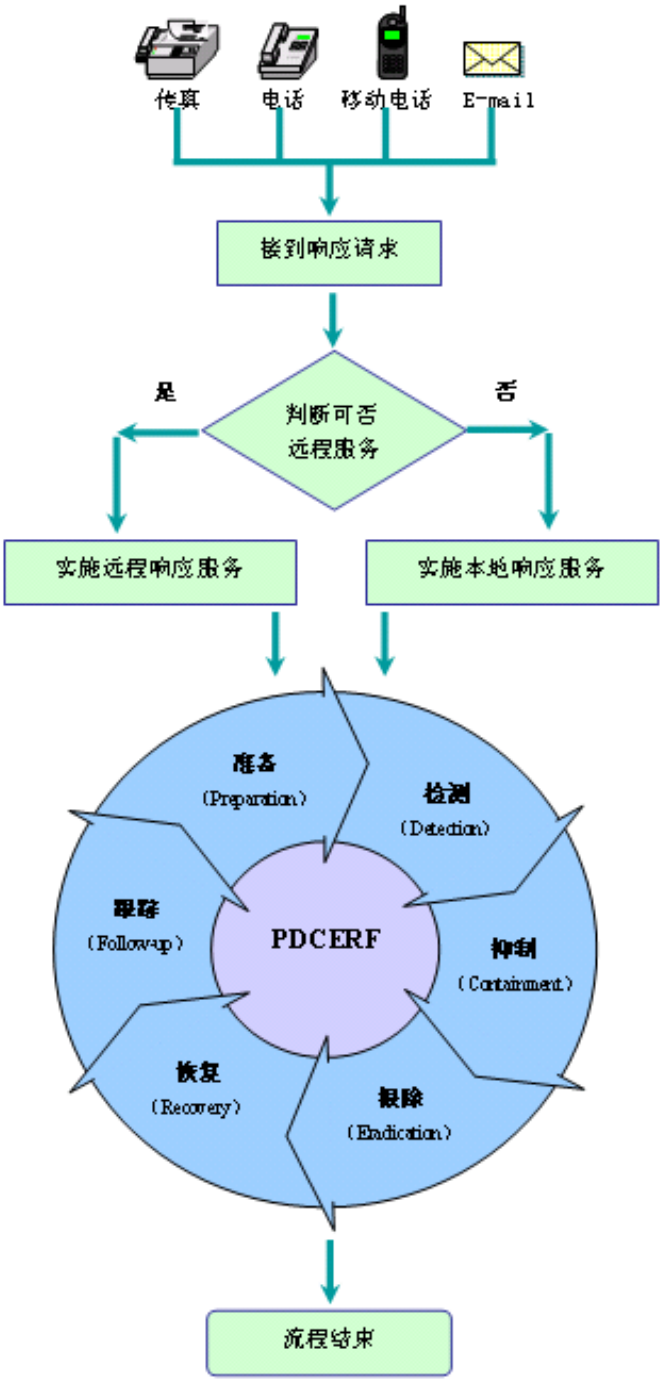
当从客户处接收到异常事件报警之后，东软的应急响应小组将通过应急响应负责人调动东软包括积极防御研究中心、入侵检测以及其他支持部门的各种资源。

第二阶段： 事件分析与处理

应急响应小组将对事件进行初步分析（现场分析和远程分析），并根据实际情况提供远程响应服务或本地响应服务。然后根据获得的事件资料分析并确定更进一步的信息获取办法，比如提供监控特征、设置蜜罐捕获系统等。在获得相关信息（比如完整异常数据包、蠕虫病毒样本、相关日志信息等）后进行全面的技术分析，同时调整相应的数据获得办法。

第三阶段： 事件结论与通告

在全面的分析处理之后，应急响应小组将向客户提供详细的安全事件通告、安全事件应急响应处理报告、事件详细技术分析文档。并根据需要提供相应工具。



3.1 详细实施流程及方法

3.1.1 预先准备与计划

- 基于该事件可能的威胁建立一组合理的防御和控制措施方案
- 确定处理问题必须的组织和人员
- 启动文档记录，服务操作的每一步都必须详细记录，包括由何人收集、如何收集、何时收集以及何人进行了访问。
- 建立一个支持事件响应活动的基础设施
  - ✧ 独立和安全的物理环境
  - ✧ 优先的网络访问通道与权限
  - ✧ 充足的应急资源（各种利用工具、备份介质、监控系统等）

3.1.2 检测与分析事件

- 迅速创建 2 份完整系统备份（一份用来充当日后的举报证据，一份可用来做系统恢复）
- 初步评估：
  - ✧ 确定事件是已经发生了还是在进行当中
  - ✧ 根据严重程度和安全策略，判断是否需要通过让受影响的系统脱机将其隔离起来
  - ✧ 估计事件的范围
- 查找黑客踪迹
  - ✧ 检查审计日志是否存在异常活动（不正常连接、安全审计失败，失败的登录尝试，非工作时间的活动）、日志不存在或日志有空缺
  - ✧ 检查黑客工具（密码破解工具、特洛伊木马等等）
  - ✧ 文件、目录和共享权限的更改
  - ✧ 检查是否有未经授权的应用程序被配置为自动启动

- ✧ 检查帐户是否权限提高或有未经授权的组成员
- ✧ 检查是否有未经授权的进程
- ✧ 检查防火墙、IDS 等系统日志

- 扫描系统漏洞
- 记录所发生的事件
- 确认事件：
  - ✧ 确定是否属于安全事件
  - ✧ 确定攻击的类型、方式及严重程度
  - ✧ 确定攻击来源与意图
  - ✧ 识别所有受攻击的系统。如果发现其他系统，请重新调用检测步骤
  - ✧ 重新评估，如果必要，可以给事件重新指定优先级别
- 如有必要，通知 NCSIRT 联络员寻求其它 IT 部门的技术支持与帮助
- 如有必要，通知信息交流官员寻求其它单位组织（例如 ISP 接入商）的帮助

3.1.3 信息取证与追查

- 系统状态分析：
  - ✧ 帐号、口令
  - ✧ 后门、木马
  - ✧ 遗留文件
  - ✧ 配置或权限改动
  - ✧ 受损文件、数据
  - ✧ 针对基准比较受损后的系统性能
- 日志提取：
  - ✧ 系统日志
  - ✧ 防火墙日志
  - ✧ 入侵检测日志

- ✧ 其它日志审计

- 设置诱饵服务器作为陷阱
- 反向探测攻击者来源
- 如有必要，通知 NCSIRT 联络员寻求其它 IT 部门的技术支持与帮助
- 如有必要，通知信息交流官员寻求其它单位组织（例如 ISP 接入商）的帮助
- 确定证据是否得到保护

3.1.4 通告发生的事件

- 将检测与取证结果传达给 NCSIRT 联络员、信息交流官员和用户方有关的主管人员。
- 通知其它适合的机构，比如：
  - ✧ 国家计算机网络应急技术处理协调中心(http://www.cert.org.cn/)
  - ✧ 国家计算机网络入侵防范中心（http://www.nipc.org.cn/）
- 如有必要，根据法律顾问的指导，通知本地有关执法部门。

3.1.5 修复与加固受损系统

- 出具修复建议方案，并进行模拟测试，提交测试结果，在得到用户方的认可后方可进行后续工作。
- 考虑用新硬盘重建一个全新的系统（应将现有的硬盘卸下并保存起来，因为在决定起诉攻击者时它们可以作为证据）。
- 修改所有防火墙和路由器的过滤规则，拒绝来自疑似发起攻击的主机的所有的流量
- 封锁或删除被攻击的登陆帐号
- 确保所有本地系统与服务的密码都换成与攻击发生之前不同的密码。还应更改其它相关主机的帐户密码。

- 关闭或修补被利用的服务与配置
- 清除攻击方遗留下来的后门、木马等文件
- 复原被篡改的文件权限与配置
- 加固系统与服务配置，去除其它安全隐患
- 提高系统或网络行为的监控级别
- 利用经过验证的最近未受影响的备份有选择地把受侵害或被破坏的系统、应用、数据等还原到它们正常的任务状态
- 建立系统文件完整性校验数据库，并保存在安全的地方。在每次系统文件正常更改后建立新的完整性校验数据库。
- 验证系统功能，并根据历史基准数据比较系统性能
- 如有必要，通知 NCSIRT 联络员寻求其它 IT 部门的技术支持与帮助
- 如有必要，通知信息交流官员寻求其它单位组织（例如 ISP 接入商）的帮助

3.1.6 监控与审查系统运行状况

- 在安全应急事件处理完成后的 72 小时内，服务工程师根据需要从远程或本地继续监视客户系统运营情况（主要监视重复性攻击和由于遏制步骤所导致的错误配置），确保故障根本上得到解决，并填写监控报告。

3.1.7 总结报告与更新安全策略

- 将所有笔记、记录汇编成一份综合性安全意外事件活动日志。
- 分发给意外事件的参与者，以便审查和批准。（包括适用于司法的证据）。
- 审查违反安全的原因，改善预防措施，防止未来再发生的意外事件和相关攻击。
- 为管理或法律目的收集损失统计信息，帮助财务部门评估违反安全造成的代价。

- 给管理层和其他关键人物准备报告，以解释事件发生的原因、违反安全造成的代价以及未来如何预防。
- 帮助客户更新和完善现有信息安全策略。

从 2000 年至今，东软安全服务团队已经通过多种方式为电信、银行、证券、政府、企业等客户提供了不同级别的应急响应安全服务，并且得到了客户方100%的好评率支持。东软始终坚持“软件创造客户价值”的经营理念，以“客户为中心”为客户提供诚信、可靠、全面的服务和解决方案，真正实现客户的价值。我们始终围绕客户价值、通过技术创新来为客户提供满意的服务和支持，帮助客户保障大型和复杂业务网络系统的安全。

4 东软应急响应服务资质及案例

4.1 应急响应服务资质

4.2 服务案例

编号	客户名称	实施时间	实施地点	服务内容

1	吉林移动	2002 年 4 月	长春	运行移动短信网关平台的系统 Solaris8 被入侵植入 rootkit,经判断攻击者利用/bin/login 存在通过客户端本地环境变量 TTYPROMPT 绕过验证漏洞取得权限；通过打补丁，去 suid 等多种手段加固主机；并使用防火墙、入侵检测等进行审计、加载访问控制策略。定期远程对主机系统进行监控和安全评估。
2	山西移动	2002 年 10 月	太原	运行移动短信网关平台的系统 Solaris8 的 oracle 用户存在弱口令 oracle，被攻击者探测到后，利用权限提升 gsu2 得到 root 权限，植入 rootkit;通过打补丁，去 suid 等多种手段加固主机；并使用防火墙、入侵检测等进行审计、加载访问控制策略。定期远程对主机系统进行监控和安全评估。
3	辽宁铁通	2002 年 12 月	沈阳	利用 Nemesis（复仇女生）利用存在 unicode 和二次解码漏洞的数以万计的服务器执行 ping –l 30000 –n 2048 目标 IP 地址，将辽宁铁通的出口网络带宽全部消耗，损失上百万元；东软配合辽宁省公安厅经过几周的追查将攻击者抓获。用户网络恢复正常，东软同时为用户提供其他安全服务。
4	甘肃烟草	2003 年 10 月	兰州	用户的网络内存在大量的木马和蠕虫，频繁造成网络故障；同时由于部分网络设备选择不合适，在流量稍大的时候成为网络瓶颈；此次服务内容主要帮助用户分析和解决问题，进行网络拓扑和性能的调优。

5	北京城建集团	2003 年 11 月	北京	webserver 主服务器及其他网络服务器被种植木马、后门、黑客工具，系统配置被篡改。东软的安全应急响应包括清除系统中各种黑客工具、后门程序、后门帐号等，安全补丁修补、系统加固、网络恢复等。
6	南通电信	2003 年 11 月	南通	南通电信的两台 DNS 服务器遭受到以 udp 为载体的进行递归查询的拒绝服务攻击，造成 adsl 用户不能正常上网，遭到投诉；此次服务主要帮助用户对 bind8.2 进行配置的优化，并通过 ndd 配置网络参数对服务器的抗 DOS 攻击能力进行加强。
7	天津网通号簿公司	2003 年 12 月	天津	天津网通号簿公司天津黄页首页遭到替换，服务器为 Solaris7；攻击者利用 sendmail 漏洞侵入，添加超级用户 r00t,并植入多个 rootkit；服务内容：对主机进行加固，并远程监控。
8	广西联通	2004 年 4 月	南宁	广西联通 IDC 的业务网站、如意邮服务器、飞时通 WEB 网站遭受 DDOS 攻击。东软的安全应急响应服务包括：协助恢复系统正常工作，系统安全评估、加固，入侵事件的调查分析，系统运营跟踪维护等。
9	山东高检	2004 年 4 月	济南	山东高检门户网站遭到入侵，网站主机桌面上被放置上”黑客”留言警告文件；原因是网站 sqlserver 的 1433 端口由于网站开发人员远程开发的需要而开放，结果 sa 口令为空，导致攻击者进入。服务内容：排查系统是否存在木马等恶意代

				码；加固主机，修改 mssql 开放端口；配置防火墙限制可访问数据库 IP 等
10	沈阳铁通	2004 年 5 月	沈阳	Phatbot 病毒爆发，由于其传播地址为从本地地址推导 B 和 C 类地址，造成汇聚层交换机满负荷，正常用户不能上网。服务内容：进行流量分析，把 TOP 10 病毒感染用户从网络上隔离；经过 1 小时之后，使网络恢复正常。
11	长庆油田	2004 年 6 月	西安	上万台接入 PC 由于用户安全意识差，蠕虫泛滥，并因此导致网络性能很差。 此次服务内容主要为：排除网络安全问题，对重点服务器加固，重新制定访问控制策略。
12	兴业银行总行	2004 年 7 月	福州	因某些国外敌对势力对我国金融体系特别是网银系统的破坏企图，对兴业银行总行的网络银行核心系统进行安全评估，主要进行恶意代码的分析。
13	浙江电力	2004 年 8 月	杭州	Apache Web 服务器被攻击入侵。东软的安全应急响应包括：系统恢复，补丁修补、系统加固，事件分析，安全防护建议等。
14	大连水产学院	2004 年 9 月	大连	欺诈网页事件、主机被入侵事件的调查分析，安全防护建议等。

15	东方卫星通信	2004 年 9 月	北京	运营 OA 系统运行某一业务时变的非常慢；经过排查发现该业务运行时用到的某个控件试图访问其主页进行更新；而此时域名服务器不可用（以前可用），导致超时的原因时该控件试图解释其访问的域名。
16	辽宁省气象局与辽宁移动合作气象短消息服务器	2004 年 10 月	沈阳	服务器被恶意攻击者添加诱骗网页，伪装花旗银行主页盗取用户敏感信息。东软公司的安全应急响应包括：清除恶意网页，排除服务器的不安全设置，并清除攻击者上载的恶意程序代码，事件分析报告，安全防护建议;将此信息报告给 CNCert。
17	青海省气象局与青海移动合作气象短消息服务器	2004 年 10 月	西宁	服务器被恶意攻击者添加诱骗网页，伪装花旗银行主页盗取用户敏感信息。东软公司的安全应急响应包括：清除恶意网页，排除服务器的不安全设置，并清除攻击者上载的恶意程序代码，事件分析报告，安全防护建议；将此信息报告给 CNCert，并集合辽宁案例继续判断是否为 Botnet。
18	江西省委党校	2004 年 12 月	南昌	首页被黑，主要内容为侮蔑管理员技术能力低下；经过分析发现网页的某一个连接指向的论坛采用的系统为 DvBBS7 存在注入漏洞；并在主机上发现攻击者上传的 ASP 木马：桂林老兵的 ASP 站长助手 6。我们建议用户替换论坛，并对其他 asp 页面进行注入检查，也发现了其他高风险的注入点，对用户的 asp 代码进行防注入修改。

19	公安部	2005 年 5 月	北京	公安部门户网站 www.mps.gov.cn 遭受分布式的 tcp 拒绝服务攻击。 我们的工作内容： 提供防火墙利用审计和黑名单的功能将攻击防住，同时利用实时监控不断的检测系统运行。同时配合公安机关进行取证。
20	国家安全生产监督管理局	2005 年 7 月	北京	网络中部分主机感染蠕虫，使得整个网络遭受蠕虫攻击，导致网络瘫痪。经分析发现感染了集 IRC 后门、蠕虫功能于一体最新的病毒。东软公司的安全应急响应包括：定位感染主机，提供清除蠕虫病毒解决方案，修复多台感染主机，并提供主机安全防护建议。
21	天津烟草专卖局	2005 年 12 月	天津	天津烟草专卖局市局及 15 个分公司同一时间感染多种新型蠕虫病毒，整个网络及业务面临瘫痪，使用最新版的杀毒软件也无法查杀。东软应急响应小组接到通知后迅速赶赴市局及 15 个分公司现场，采用人工手动方式进行分析和查杀，并为受感染主机进行加固，第二天网络及业务恢复正常。此次应急响应得到了客户的高度评价。
22	公安部	2008 年 6 月	北京	2008 年 6 月，公安部全国公民身份证号码查询系统遭受恶意 DDOS 攻击，我方迅速指派技术人员赶赴现场，在配合使用 Ntars 异常流量监控与响应系统的基础上，在最短的时间内将 DDOS 流

				量迅速降低下来，并恢复了网站系统的正常访问。
23	广东省地税局	2009 年 2 月	广州	2009 年 2 月，广东地税向多家安全公司（其中包括东软）发出应急支援请求---广东地税的多台内网服务器出现文件共享访问故障，IDS 产生大量暴力口令猜解报警，怀疑受到了恶意人为攻击。东软公司迅速指派安全服务技术人员赶赴现场，在其它几家安全公司检查未果的情况下，我方经过详细排查和深度挖掘，最终发现为一种新型蠕虫病毒所为，该病毒具有极强的隐蔽性，并利用 ms08-067 和 09 年最新的 ms09-001 系统漏洞以及系统弱口令帐号进行传播感染，并嵌入在 server 服务的通讯通道中。在定位事件故障原因后，我方对故障服务器进行修复使之恢复正常，该事件的响应和处理得到了广东地税的高度赞扬。
24	陕西广播电视局	2009 年 10 月	西安	2009 年 10 月，我方接到用户求助，对方网站被挂马，东软立刻派出安全工程师进行远程网站检测，发现网页中均被嵌入非法网址，经过服务器检查，未发现异常，进过反复对网页挂马检测，未发现服务器植入木马等现象，随后东软将调查重点放在数据库里，最终发现数据库异常，经过删除垃圾数据，升级补丁的方式恢复了网站的正常运营，得到用户好评。
25	中投公司	2010 年 2 月	北京	2010 年 2 月，我方接到中投公司求助，IDS 多次报警 yessky 病毒，经过我方工程师到实地调

				查，发现其中一台机器感染病毒，并不停向外发送信息，经过清除，网络恢复正常，得到用户肯定。
26	上海航空	2010 年 7 月	上海	我方接到上海航空求助，积分兑换网站积分被恶意兑换，我方立刻派出工程师远程监测，发现该网站存在测试页面，且为管理员权限。经过扫描，发现服务器本身并无漏洞，但通过进一步分析，发现存在业务安全隐患，即默认情况下，用户账号和口令存在规则性。我方立刻通知用户，避免了更大范围的扩散，得到用户充分肯定。
27	南方电网	2010 年 8 月	广州	在项目实施期间，我方发现某调度网中 SOC 频繁报警存在异常登录事件，我方高度重视，立刻派工程师前往处理，经过分析日志，发现登录频率非常高，不可能是人为的，故初步判定是机器感染蠕虫或病毒，定位具体机器后，迅速清除了病毒，网络恢复正常，该事件由于发现及时，为用户亚运保障作出了贡献，得到一致好评。
28	国际航空	2011 年 4 月	北京	我公司接到国际航空网络中断异常，经过现场与国航工程师共同分析，通过调查发现来自某 IP 的流量异常，经过详细分析日志，果断调整边缘路由、IPS 和黑洞抗 DDOS 攻击设备，使得安全事件得到缓解，为了根本解决该问题，我公司提出了完整的安全建议。
29	东方航空	2011 年 5 月	上海	我方接到用户报告，东方航空常旅客系统被人恶意篡改积分，且通过积分成功订购机票。

				我方立即组织安全专家现场调查事故发生原因，并对应用系统进行排查，对庞大日志信息进行分析，最终得到攻击人员的信息，为立案提供了最直接的证据，得到东方航空领导的表扬。
30	广东省地方税务局	2011 年 5 月	广州	经检查发现非法用户 2010 年 6 月 2 日注册了 www.yvzhou.com 国际域名，并将自身域名重定向到省地税网站。我方提出网站域名规范及互联网统一出口方案并实施。
31	东方航空	2011 年 8 月	上海	我方接到用户报告，东方航空网站被人攻击，所有页面数据被清空。 我方立即组织安全专家现场调查网站所在的服务器、网络设备等有可能留下攻击人员蛛丝马迹的地方，最终发现由于网站系统采用了不安全的功能组件，导致被攻击人员利用，进而进入后台，把整个数据库清空。 并且成功查找到攻击人员来源，为实施解决措施提供了直接材料，得到了用户的表扬。
32	华侨城集团	2011 年 7 月	深圳	我方接到用户报告，邮箱账户存在异常登录事件，我方立刻组织工程师远程检测，发现系统存在大量弱口令，经过我方建议，用户关闭了远程访问并及时设置口令复杂度，由于我方快速响应并迅速定位问题，及时处理用户问题，得到用户的肯定。

33	启德教育集团	2011 年 8 月	广州	我方接到用户报告，启德教育集团通信服务器出现服务器响应异常，服务器无响应。 我方立即组织安全专家赴现场对服务器进行故障排查，发现服务器无响应是由于应用软件故障导致，通过联系应用软件开发厂商并部署 UTM 设备解决问题。
34	东方航空	2011 年 11 月	上海	我方接到用户报告，东方航空报表服务器出现异常，应用程序无法工作。 我方立即组织安全专家对报表系统所在的服务器、数据库服务器等进行安全检查、日志分析、访谈等工作。最终发现由于人员安全意识不强，导致该服务器中了恶意程序，应用程序无法正常通讯，导致报表应用系统无法启动的现象。
35	广东省地方税务局	2011 年 12 月	广州	我方接到用户报告，省地税在线发票业务系统应用系统与加密机之间通讯终端，出现业务中断现象。 我方立即组织安全专家赴现场对服务器进行故障排查，经检查发现目前网上报税系统各应用主机、边界防火墙、加密机、数据库主机，全部部署在核心交换机下。 业务应用系统与安全应用系统间的通讯设置了 3 秒超时，安全应用系统在访问加密机时如连接失败不会自动丢弃当前连接，采用继续生成新的连

				接。 网络设备性能检查无异常，网络数据包和流量，没有故障时间的的实际数据无法分析，IDS 没有发现有针对系统各主机的攻击，运维人员重新启动业务系统各主机后故障消失，根据以上检查结果分析为业务系统设计缺陷，软件开发部门修改后应用系统与加密机之间通讯连接机制后问题解决。