**说明：具体实施基本流程及技术服务内容会因不同客户需求、环境而有不同，请以具体订单的原厂和用户的双方约定为准。**

**以下提供一般情况下的流程供参考：**

**项目实施基本流程：**

1）RSA发送配置表格给用户填写，配置表格包括邮件地址，网络日志收集详细信息，联系人详细信息等；

2）用户发送填好的配置表格反馈给RSA；

3）RSA根据用户的需求配置架构，大约需要两三个星期；

4）用户开始发送网络日志（web log）或钓鱼网站邮件给RSA反钓鱼指挥中心（ AFCC）做进一步调查。

**技术服务内容**

RSA反钓鱼技术服务内容包括以下内容：

|  |  |  |
| --- | --- | --- |
| 序号 | 服务内容 | 描述 |
| 1 | 实时警报和检测 | 基于各种探测器和品牌监视技术，每天扫描超过10亿封电子邮件以及大量的域名和聊天室 |
| 2 | 报告 | 指挥中心使用预定义的统计、建模等工具对攻击进行评估，并相应将更新的报表发给各家金融机构。 |
| 3 | 站点封禁网络 | 与AOL、Netscape、EarthLink、Microsoft及其他多家大型企业合作，可以帮助确保1亿多位网络用户不会访问到那些经过确认的钓鱼站点。 |
| 4 | 关闭站点 | 反钓鱼指挥中心(AFCC)的会诊室(war-room)会负责联系网络服务提供商，协同他们关闭用于欺诈的站点。在过去两年中，AFCC已经关闭了超过8000个欺诈站点。 |
| 5 | 鉴定工作 | AFCC的反钓鱼专家会对攻击进行鉴定分析，并尝试提取出其他有用的信息。 |
| 6 | 应对措施 | 包括一系列正在申请专利的工具，可以帮助降低攻击的危险性，同时将攻击所造成的影响降至最低，并阻止欺诈者发动后续攻击。 |
| 7 | 防止域欺骗 | 在检测阶段实现对DNS中毒和DNS欺骗攻击的保护，并关闭所有受DNS欺骗攻击影响的站点。 |
| 8 | 可选的标志监视、品牌保护 | 使用相应技术连续不断地扫描网络，查找含有企业名称或品牌标志的图片，提供额外的保护层。 |

感谢！