金融是影响国计民生的重要行业，中央办公厅、国务院办公厅、公安部、人民银行、银监会、证监会和保监会等主管部门对金融系统的信息安全问题非常重视，先后对金融行业信息安全工作提出了指导建议和相关规定，明确指出要加大在信息安全治理工作方面的投入，特别是要保障对公众提供服务的业务系统的安全性和可靠性。

以下是近年来各监管部门出台的一些指导建议和相关规定。

|  |  |  |  |
| --- | --- | --- | --- |
| 主管部门 | 文号 | 日期 | 文件名 |
| 中央办公厅和国务院办公厅 | 中办发[2003]27号 | 2003年8月 | 国家信息化领导小组关于加强信息安全保障工作的意见 |
| 中办发〔2006〕18号 | 2006年5月 | 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 |
| 国务院办公厅 | 17号文 | 2008年 | 关于加强政府信息系统安全和保密管理工作的通知 |
| 公安部、国家保密局、国家密码管理局和国务院信息化工作办公室 | 公通字[2004]66号文 | 2004年9月 | 关于印发《关于信息安全等级保护工作的实施意见》的通知 |
| 公通字[2007]43号文 | 2007年6月 | 关于印发《信息安全等级保护管理办法》的通知 |
| 公信安[2007]861号 | 2007年7月 | 关于开展全国重要信息系统安全等级保护定级工作的通知 |
| 银监会 |  | 2006年3月 | 《电子银行业务管理办法》和《电子银行安全评估指引》 |
| 银监发[2006]63号 | 2006年11月 | 关于印发《银行业金融机构信息系统风险管理指引》的通知 |
| 银监办通[2006] 313号 | 2006年11月 | 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 |
|  | 2007年6月 | 中国银监会关于印发《商业银行操作风险管理指引》的通知 |
| 银监办发[2007]134号 | 2007年6月 | 关于做好网上银行风险管理和服务的通知 |
|  | 2008年3月 | 关于开展银行业金融机构信息科技风险奥运专项自查工作的通知 |
| 中国人民银行 | 中国人民银行公告〔2005〕第 23 号 | 2005年10月 | 电子支付指引（第一号） |
| 银发[2012]121号 | 2012年5月 | 中国人民银行关于发布《网上银行系统信息安全通用规范》 |
|  | 2012年12月 | 中国金融移动支付标准 |

监管政策的要求和日益严峻的网络安全现状要求我们加大安全防护力度，并开展定期的安全咨询与评估工作。

**服务介绍**

应急响应范围包括网络或系统中的计算机或网络设备系统的硬件、软件、数据因非法攻击或病毒入侵等安全原因而遭到破坏、更改、泄漏造成系统不能正常运行，或已经发现的有可能造成上述现象的安全隐患。

包括以下情况，都属于安全事件：

- 非授权访问，通过入侵的方式进入到未被授权访问的网络中，而导致数据信息泄漏；  
- 信息泄密，数据在传输中因数据被截取、篡改、分析等而造成信息的泄漏；  
- 拒绝服务，正常用户不能正常访问服务器提供的相关服务；  
- 在系统日志中发现非法登录者；  
- 发现网络大面积爆发计算机病毒感染；  
- 发现有人在不断强行尝试登录系统；  
- 系统中出现不明的新用户账号；  
- 管理员收到来自其它站点系统管理员的警告信，指出系统可能被威胁；  
- 文件的访问权限被修改；  
- 因安全漏洞导致的系统问题；  
- 其它的入侵行为。

安全事件根据事件危害程度可以分为：

- 严重安全事件：XXX电子银行系统由于安全原因崩溃、系统性能严重下降，已无法提供正常服务，出口路由由于网络安全原因非正常中断，严重影响用户使用，公众服务由于安全原因停止服务或者造成恶劣影响的。

- 普通安全事件：由于安全原因导致系统出现故障，但不影响用户正常使用，XXX提出安全技术咨询、索取安全技术资料、技术支援等。

**服务级别**

根据项目我方提供的应急响应级别如下：

1. 事件处理响应时间：在10分钟内客户能够联系到安全服务方，并且安全服务方对于安全事件问题的解决给予答复。

2. 事件处理到场时间：严重安全事件：3小时；普通安全事件：远程协助，必要时到场。

3. 事件初步处理时间（指受影响的通信或者业务恢复网络通信的状态，不包括系统或数据的恢复工作和时间）：严重安全事件：3小时；普通安全事件：一个工作日。

4. 事件最终处理时间：

安全事故：24小时；  
严重事件：24小时；  
普通安全事件：三个工作日。  
  
  
安全服务方需针对常见的安全事件及XXX相关单位现有信息系统现状制定应急方案，应急方案通过XXX相关单位审批后，定期进行一次模拟演练。演练包括发现问题，应急反应，恢复等内容。

安全服务方在处理安全事件过程中，可以通过分析网络数据、检查系统或应用软件相关参数、病毒分析等多种技术措施和手段掌握事件相关信息，但要在进行事件恢复操作之前，需对相关情况做书面记录和电子文档记录；同XXX相关人员商议、确认后，才可以进行。

**服务内容**

1.文档审阅：审阅评估对象的网络拓扑、设计、开发、安装配置、运行维护、安全管理等文档。

2.代码审阅：通过专业化的源代码安全检查，发现应用系统现有的和潜在的安全问题。

3.人员访谈：与各评估对象的相关人员进行沟通交流，弥补文档审阅等的不足，进一步了解各评估对象的信息。

4.脆弱性扫描：使用脆弱性扫描软件对各设备（包括其上所安装的各关键软件）进行扫描。

5.本地审计：使用启明星辰本地安全审计工具包、命令行等方式收集各设备可能存在的技术脆弱性信息，以便在分析阶段进行详细分析。

6.现场观测：观察与应用系统安全有关的机制、配置现状；现场巡视机房室内室外实际环境。  
  
  
**服务流程**

启明星辰为事件响应建立自己的流程规范，经过多次的响应实践证明其可行有效。我们提供的漏洞检测服务、监控审计服务、DDOS防御服务都是在为事件响应提供事件处理所需的原始资料，一旦事件发生， 事件响应小组分析的依据大部分来源于上述数据。 还将协助服务对象组织建立应急上报和联络机制，以保证在安全事件发生时，能及时得到上级主管的指导并及时联系到本组织相关人员和事件响应人员。

事件响应必须遵循的流程分为以下步骤：

第一步：记录日志

当发生安全事件时，首先需要客户对环境现场进行记录，对事件的影响进行详细的描述。安全事件日志对于安全事件的识别、处理和调查非常重要，安全事件可能在其刚刚发生时就暴露，也可能在发生的过程中或发生以后才被发现，因此所有安全事件都应该有一份书面的经过调查证明足够客观的日志，而且应该把日志妥善保存以免被修改。由于在线日志很容易被修改和删除，所以手工记录是必要的。

应该记录的信息有：

- 相关事件发生（或者发现）的日期和时间；  
- 值班人员或事件协调小组通知的人员和与事件相关的人员；  
- 受影响的系统名称（或IP地址），受影响的程序和网络；  
- 事件发生时对系统、程序或者网络的影响和现象。

记录完安全事件后，应该把安全事件上报给直接主管，同时提交事件响应申请给 的事件响应小组，此时开始进入事件响应过程。

第二步：分析确认

接到事件响应申请后， 事件响应小组会根据情况进行远程和现场的响应。事件响应小组会根据客户记录的安全事件描述，结合前期进行过的漏洞检测与分析结果、实时监控与审计结果等已有客户系统和网络状况，进行分析和判断，如果是典型的已知安全事件，部分案例可以仅通过远程方式就能解决。

如果通过远程指导客户无法进行自行解决，事件响应小组成员会赶往现场进行实际问题解决。这时，事件响应小组可以实地看到安全事件的形态和影响，也可以通过工具直接进行测试，结合当前扫描、探测、实时监控和审计的结果进行分析，可以更容易定位出问题所在。

第三步：事件处理

事件响应小组最主要的任务就是维持或恢复组织的运作。因此，一旦发生意外事件，如何防止攻击或损害事件的扩大是其主要的目标，相关人员在现场或者远程依照不同事件类型进行事件处理。

在事件处理过程中有一些重要决策可能必须要做：

1. 是否要关闭或重启系统？

2. 是否要中断系统的网络连接？

3. 是否要关闭一些特定的服务，如Telnet、FTP等？

4. 是否要调整网络设备或安全产品的策略配置？

5. 是否需要国家网络安全机构协助处理？

某些处理办法可能会暂时影响到组织的业务运转，但都是为了避免安全事件事态的扩大，这也是在第一步中要把安全事件上报给上级领导的原因，事件处理过程中可能会带来一定的风险，需要和组织主管进行协商，确定风险可以接受才能真正实施事件处理方法。事件处理过程中，要对每个处理的动作进行详细的记录。  
  
第四步：系统恢复，防御

在抑制住了攻击或损害事件的扩大以后，就要对系统进行恢复，使客户业务重新运转。如果系统在故障点有备份，被攻击的系统就用备份来恢复；应该从系统中彻底删除诸如受到感染的文件；如果调整了网络或安全产品，要把所有安全上的变更作记录。

第五步：事后分析与跟踪

在安全事件处理完毕，所有系统恢复正常以后，应该针对事件进行分析。集中所有相关人员来讨论所发生的事件以及得到的经验教训，并对现有的一些流程进行重新评审，对不适宜的环节进行修改。  
在安全事件处理后的一段事件内，应该密切关注系统恢复以后的安全状况，特别是曾经出问题的地方。  
  
  
**服务原则**

- 实时原则

- 规范性原则  
- 最小性原则  
- 保密性原则

**服务时间**

启明星辰提供7×24小时的网络信息安全事件的应急响应和技术支持，以及相关问题的深入分析和必要的整改建议，如有必要需提供现场服务，响应时间要求如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **事件级别** | **事件类型** | **响应时间** | **到现场时间** |
| 紧急 | 网络信息安全事件导致系统瘫痪、系统性能严重下降、大批量数据泄露或巨大经济损失等情况。 | 即时电话响应 | 3小时 |
| 严重 | 网络信息安全事件导致系统部分重要功能失效、系统性能明显下降、较大量数据泄露或较大经济损失等情况。 | 即时电话响应 | 5小时 |
| 一般 | 网络信息安全事件导致系统部分非重要性功能失效、系统性能稍微下降、小量数据泄露或较小经济损失等情况。 | 即时电话响应 | 8小时 |
| 轻微 | 网络信息安全事件导致系统轻微故障，没有发生数据泄露或经济损失。 | 即时电话响应 | 24小时 |

注：“到现场时间”以行方向启明星辰项目组明确提出现场支持服务需求之时起计算。