XX有限公司

2022-2023年度重保项目服务方案

XXX股份有限公司

2022年1月

目录

[1 重保项目技术支持与服务方案 1](#_Toc94098288)

[1.1 重保值守服务 1](#_Toc94098289)

[1.1.1 外网安全监测分析 1](#_Toc94098290)

[1.1.2 内网安全监测分析 11](#_Toc94098291)

[1.1.3 应急响应 16](#_Toc94098292)

[1.1.4 威胁情报 26](#_Toc94098293)

[1.2 重保总结服务 28](#_Toc94098294)

[1.2.1 复盘总结服务 28](#_Toc94098295)

[1.2.2 安全优化整改服务 28](#_Toc94098296)

# 重保项目技术支持与服务方案

## 重保值守服务

### 外网安全监测分析

按照客户要求，对恶意攻击进行分析和溯源，溯源应能定位到攻击者真实IP或物理位置，尽量获取攻击者个人信息（姓名、照片、手机号、qq号、微博账号及其他个人信息）。协助在最快时间调整安全防护策略（含技术方面和人员方面），降低重要资产因安全风险造成的损失。溯源结束后，整理形成攻击溯源报告，保留证据，协助向公安机关报案。

#### 网站监测

xxxx公司对客户互联网业务系统所面临的数据窃取、后门植入、网站恶意篡改、安全配置错误、漏洞溢出、非法越权、暴力破解、信息探测、分布式拒绝服务攻击（DDoS）等恶意攻击行为进行监测，对攻击过程进行记录，每周例行向客户发送监测报告。发生恶意攻击行为，应通过电话、短信、邮件等方式及时通知客户相关人员。

##### 监测范围

监控范围包括总行互联网出口IP地址和外网系统URL，项目执行期间，如客户出口IP地址和外网URL发生变化，监控访问也需相应调整。

##### 服务内容

###### 网站扫描

监测平台集成了网站扫描功能，该功能继承了xxxx公司明鉴网站弱点扫描器的所有优点，可以实现快速、准确的定位出网站存在的问题，并且具有丰富的可配置接口便于配置个性化的扫描要求。监测平台中的网站扫描功能主要优点如下：

智能、快速的深度漏洞扫描

采用强大的过滤模块，过滤掉重复或者不必要的网页链接，提高运行效率。单引擎单位时间的发包速率的可控化，可以有效防止扫描数据量过大影响网站正常运行的问题。扫描数据实时存储，扫描过程中实时存储扫描数据和结果，不管是由于程序自身引擎中断、进程人为关闭，还是机器断电引起扫描中断，扫描数据都不会丢失，可以进行断点续描。扫描引擎与扫描界面分离，一个正在运行的主程序可以同时管理多个引擎。每个引擎可支持多个任务的真正并发扫描，有效提高系统深度扫描速率。

全面、准确的应用弱点检测

* 支持OWASP TOP 10等主流安全漏洞（A1-注入攻击、A2-失效的身份认证和会话管理、A3-跨站脚本（XSS）、A4-失效的访问控制、A5-安全配置错误、A6-敏感信息泄露、A7-攻击监测与防护不足、A8-跨站请求伪造（CSRF）、A9-使用含有已知漏洞的组件、A10-未受有效保护的API）：SQL注入、XSS跨站脚本、伪造跨站点请求（CSRF）、隐藏字段、表单绕过、AJAX注入、弱配置、敏感信息泄漏、HI－JACK攻击、弱口令、Xpath注入、LDAP注入、框架注入、链接注入、操作系统命令注入、Flash源代码泄漏、Flash跨域攻击、Cookie注入、敏感文件、第三方软件、其他各类CGI漏洞
* 支持国际目前主流WEB应用类型：全面支持WEB 2.0，支持各类JavaScript脚本解析 ；全面支持FLASH解析；支持WAP类及WMLScript脚本类应用系统；支持基于HTTPS应用系统的检测，能够自动获取所有必须的要素，对基于SSL传输的内容进行分析，可对网银、证券交易等基于HTTPS协议的WEB应用进行自动安全评估；支持所有类型的动态页面；支持HTTP 1.0和1.1标X准的WEB应用系统 。
* 支持基于各类身份认证方式的WEB应用的安全检测：支持基于支持包括Basic、Digest、NTLM在内的身份认证方式。支持HTTP和SOCKS代理，并支持各种代理的身份认证方式。

灵活、丰富可自定义的网站扫描模式

为扫描任务提供非常丰富的扫描选项，如爬行、检测、过滤、网络环境等，用户可根据目标扫描网站的特点以及所在的网络环境，对扫描过程进行定制：

* 扫描范围：提供当前域、当前页、子路径、整个域、全部页五种扫描范围的选择。
* 扫描模式：提供先爬行后检测、边爬行边检测、只检测和只爬行四种扫描模式的选择。
* 扫描深度：根据需要可设置扫描的深度，支持无限扫描深度。
* 执行类型：根据需要可设置任务扫描的执行时间，支持立即执行、定时执行以及周期执行。
* 调度优先级：根据需要可设置低、中、高三种调度。
* 文件后缀区分：可在扫描过程中设定不测试的文件后缀，提高扫描效率。
* 流量控制：根据实际的网络连接情况和测试目标的承受能力可开启智能流控。

###### 安全事件监测

安全事件监测原理

网页安全件事件监测在深入分析研究黑客入侵篡改手法的方式进行监测，如：UA作弊、 Referer伪造、脚本跳转等，通过上万个被黑网站的安全事件样本智能学习，版本检出率在99%。

安全事件监测的主要功能

|  |  |
| --- | --- |
| 类别 | 描述 |
| 监测范围 | 支持对网站全站的监测 |
| 监测内容 | 网站首页内的文字 |
| 取证方式 | 页面快照、页面源码 |
| 安全事件监测对比 | 方式1通过对爬行下来的页面上的特征，与特征库里的特征进行匹配，发现被篡改的页面、方式2通过浏览器ua获得两次结果进行对比，抓取被篡改的部分 |

###### 敏感词监测

采用中文关键词分析技术对网站进行敏感关键词监测，实现精确的敏感词识别，确保网站内容符合互联网相关规定，避免出现敏感信息以及被监管部门封杀。网站监测平台进行了敏感关键词的管理，同时在敏感关键词的扫描任务中，通过扫描任务结果快照能够准确定位出关键词的所在位置。

###### 可用性监测

网站安全监测平台提供三个级别的网站可用性监测功能，分别从域名可用性、网站服务可用性再深入到网站程序可用性的监测。提供HTTP+PING+DNS检测方式，较为全面的实现了网站可用性的监测功能。

域名解析可用性

任何一个解析的域名均有对应的权威DNS服务器为其提供域名解析服务，如果提供权威DNS信息的域名服务器出现故障或解析出错误的信息，将导致用户无法访问到真实的网站，例如百度网站被黑就是类似的原因导致的。

监测平台通过监测权威服务器的可用性、以及权威服务器解析IP地址是否与监测平台记录的历史基准一致来判断域名是存否发生安全问题，检测到故障时会在向网站管理员提出整改建议。

网站服务可用性

网站正常工作时会自动监听指定的TCP端口，通常是TCP 80端口，且通过HTTP协议访问时能获得一个200的响应状态码，则说明网站已经正常服务。当网站采用独立的服务器，网站内容为静态内容时使用该技术检测已经可以很好的跟踪网站的可用性了，但如果网站存在虚拟主机或复杂的应用程序时则仍不能确认网站是否正常工作。

###### 挂马及后门监测

网站监测服务提供的网页挂马的监测，其算法主要由网页恶意代码分析技术和网页行为分析技术组成。通过上述两种主要的算法使网页木马检测功能实现了误报率低、漏报率底、能发现部分未知网页木马的效果。

网站监测服务采用模拟执行、参数动态分析监测技术和后门语义分析技术，并根据webshell的行为模式构建了基于机器学习的智能检测模型。传统技术与人工智能技术相结合、静态扫描和动态分析相结合，更精准地检测出网站已知和未知的后门文件。

###### DDoS防护

针对各类业务系统发起的DDOS攻击进行流量清洗，最大防护峰值可达2.5T，采用3-4层清洗模块针对大流量DDOS、syn-flood、ack-flood、udp-flood、icmp-flood、NTP攻击进行清洗，保障在线业务系统的可用性和连续性。DDOS防护全国回源50ms以内，弹性防护，永不回源。



###### WEB防护

玄武盾提供了目前业界覆盖范围最广、防护能力最强的WEB安全防护，对Web网站或应用进行严格的保护。安全策略来自于Snort、CWE、OWASP组织，以及安恒安全研究院对国内典型应用的深入研究成果，采用机器学习+规则双重检测机制，通过机器学习识别注入和跨站类攻击。



通过规则检测引擎针对协议违规、Webshell、盗链、组件漏洞、CSRF、信息泄露等攻击进行拦截。



HTTP协议规范性检查

检查提交的报文是否符合HTTP协议框架，如异常的请求方法、不同字段的合规性、特殊字符、重点字段的缺失、HTTP方法控制、超长报文造成的溢出攻击以及对高危文件的访问等，黑客在使用非浏览器工具调试时可迅速拦截。

Webshell检测

对用户上传的文件后缀名和文件内容进行全方面检查，杜绝Webshell的上传和访问，并对已经上传的Webshell进行拦截。

注入攻击防护

对用户提交的URL、参数、Cookie等字段进行检查，采用SQL语义解析技术防止风险系数极高的SQL注入攻击，采用字符偏移技术对代码、命令、文件、LDAP、SSI等注入攻击的检测，有效地防护了对操作系统和应用的注入攻击。

跨站脚本攻击防护

采用字符差分技术对用户提交的脚本进行检查，防止不合法跨站脚本，防护存储型、反射型和DOM型跨站。

信息泄漏防护

对服务器响应状态码、服务器错误信息、数据库错误信息、源代码信息泄露进行过滤，防止服务器信息被黑客利用进行有效攻击，并对身份证、手机号等敏感信息进行脱敏处理。

第三方组件漏洞防护

对WEB服务器容器、应用中间件、CMS系统等漏洞进行有效防护。

CSRF跨站请求伪造防护

通过Referer算法和token算法有效对CSRF攻击进行防护。

防盗链

通过Referer和Cookie算法有效防止非法外链，和对用户资源内容的盗链。

CC防护

针对小流量、应用层DDOSx攻击采用专利级CC防护引擎进行识别及拦截，通过威胁情报的恶意IP库、肉机/代理主机库、扫描IP库等进行碰撞，将一部分扫描、爬虫、刷票、CC等应用层DDOS攻击进行过滤。

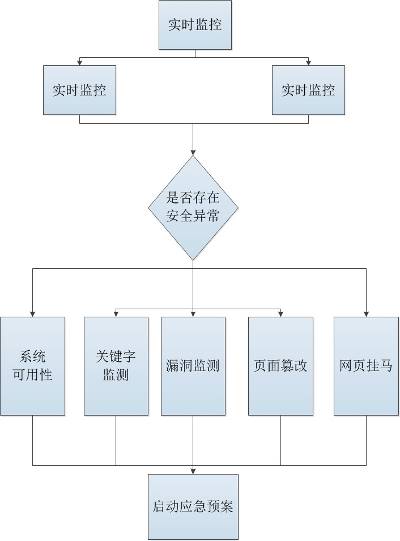
CC攻击通常具备访问频率高、集中度高等特点，通过专利级CC多重检测算法，根据用户访问频率、用户访问集中度、用户访问行为、QPS限流等多种方式进行过滤，紧急情况下可通过区域级封锁和挑战模式进行极限防护。

扫描攻击通常具备单IP访问频率高、响应错误率高、访问资源固定等特点，安恒玄武盾采用专利级行为检测算法，先对扫描器进行指纹识别过滤，再针对客户端的响应错误分布率、资源访问分布率、触发攻击概率等多种行为进行分析匹配，1分钟内完成扫描器识别并进行封锁，可拦截市面上大部分扫描器。

爆破撞库和CC攻击手法非常类似，可采用同样的防护手段进行拦截。



##### 服务流程



##### 服务优势

###### 事前安全风险扫描

未雨绸缪：针对被监管的网站，可扫描其存在的安全风险，即安全漏洞，包含OWASP TOP10以及各类0day漏洞，有助于漏洞被利用前进行安全加固，降低安全事件发生的概率

###### 事后安全事件监测

亡羊补牢：在网站发生了安全事件后，即被挂入网页木马、暗链、以及发生篡改、敏感言论等等情况，第一时间法先问题，进行应急处理，降低影响。

###### 安全监管工作落地

采用实时告警、网站安全评分、网站安全趋势、通告报表、责任到人等方法，促进安全监管工作落地，提高网站安全水平。

###### 风险通报落到实处

风险发生以后，通过短信&邮件的方式进行通告给相关责任人，无需人工发邮件或打电话通知，降低人工操作，提升通告效率，以此降低事件的影响面。

##### 服务方式

xxxx公司将派驻工程师驻守客户现场，进行7\*24监测值班工作，一旦监测到安全事件发生，将通过邮件、短信和电话等方式进行预警，及时通知、协助客户及相关人员进行事件应急处理。

##### 成果输出

xxxx公司最终输出物：定期（每天/周/项目）分析针对客户的互联网网站监测报告，并给出应对建议方案。

#### 协助处置

##### 一键关停

当网站出现紧急安全事件时，可通过手机APP和浏览器一键秒级完成全站关停，防止网站因安全事件被通报或散布到互联网上，产生不良影响，同时针对暗链、黑页等异常页面支持URL级关停。



##### 虚拟补丁

支持虚拟补丁一键下发功能。网站出现0day漏洞时能快速完成漏洞修复，为人工修复补丁和修正软件源代码都争取了时间。解决了人工修复漏洞的针对性、时效性和安全性不强的问题，大大节约了人力和运营成本，有效保障网站安全性和可用性。

##### 区域访问控制

国内的部分政务网站和业务系统基本都是所在辖区省内用户在使用或者访问，国外IP正常的访问占比非常少。所以在敏感期可以设定仅国内IP地址可以访问网站和业务系统，或者限定一些区域无法访问，可以有效降低被攻击的风险。可视化的操作界面，可精确到区县级别，点点鼠标就能完成封锁。



##### 永久在线

开启永久在线功能后，永久在线根据访问记录定期自动学习网站服务器内容。

当用户网站因为服务器故障、线路故障、电源等问题出现无法连接时，可自动切换到镜像站。在敏感期或特殊时期时，用户网站即使在主动关闭的情况下仍可显示网站页面，保证网站永久在线。



### 内网安全监测分析

安全态势感监控知是指在网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、展示以及进行趋势预测的能力。

安全态势监控技术主要包括以下内容：

* 态势认知：对网络当前状态进行理解，主要包括：状态识别与确认；状态识别是意识有攻击正在发生，状态确认包括确认攻击类型、来源、属性和攻击目标等。
* 影响评估：对当前和未来攻击的影响面、破坏力等进行多维度的评估。
* 质量评价：通过真实性、完整性和时效性，确认所收集的态势感知信息素材的质量和可信度，以及由此形成的“知识、情报、决策”的服务链。
* 评估态势发展趋势：对攻击者意图、时机和能力以及当前网络的漏洞等进行了解，并预测攻击者将来可能采取的行动、活动和路径，并给出最合理的防范手段。

综上，安全态势监控可分为三个阶段进行实现：态势识别（态势认知和质量评价）、态势理解（影响评估、攻击者行为认知、原因和方式认知）和态势预测（态势跟踪、发展趋势）。

#### 威胁情报

威胁情报值守是一种新型的、面向威胁的安全举措，它涵盖了与威胁相关的上下文、指标、攻击概况、影响及应对建议。其主要思路从传统安全防护体系的“以漏洞为中心”，推进为“以威胁为中心”。

面对当前严峻的网络空间安全形势，可通过整合用户终端、网络链路、应用系统等各类数据源，利用威胁情报的感知、共享和分析，建立纵深防御机制以对抗各类安全威胁。其核心包括：

* 利用多种渠道，采用多样化的技术手段，采集大规模碎片式的异常数据以及其他相关威胁信息。
* 通过集中的深度挖掘、提练、融合、归并以形成与信息系统核心资产有关的威胁线索集合，并结合恶意特征进行分析，得出有价值的威胁信息，为后续分析、预判、决策提供基础。
* 通过威胁情报的评估、关联分析、以及智能推演完成海量情报分析，通过支撑网络空间安全防御的计划、执行、检查及处理，形成安全防护的闭环。

威胁情报值守的分析结果可为信息及网络安全评估提供有益的支持，同时结果也可作为威胁情报一部分促进对威胁的认识，以加强对威胁的感知、处理、预测。

#### 安全大数据分析

当前网络与信息安全领域正面临着多种挑战。一方面，安全体系架构的日趋复杂，传统的安全技术难以应对安全数据体量越来越大的局面；另一方面，随着新型威胁的兴起、内控与合规的深入，需要更加快速的对安全事件进行判定和响应。

传统的分析方法大都采用基于规则和特征的分析引擎，而规则和特征只能对已知的攻击和威胁进行描述，无法识别未知的攻击，或者是尚未被描述成规则的攻击和威胁；随着大数据技术的不断成熟及应用，出现了将大数据技术应用于安全领域的大数据安全分析技术。

大数据安全分析技术将原本针对样本数据的分析拓展到针对全量数据的分析，从基于特征的匹配分析升级到基于行为的异常分析。同时大数据安全分析可以用到大数据分析的所有普适性的方法和技术，提升了机器学习、深度挖掘等算法在安全领域运用的可行性，主要可实现以下方面：

* + - 1. 确定威胁：通过确定关键业务安全需求，对威胁进行深入分析，并通过管理网络基础设施及相关的业务流程，确定系统遭受入侵及被破坏的可能性。
      2. 量化风险：在威胁确定之后，对威胁影响和概率等相关指标进行量化。
      3. 数据汇聚：对业务类数据（如资产属性、组织结构等）、网络数据（如全包捕获、会话或Flow数据等）、设备及应用的日志、报警数据（如防火墙、防病毒软件等）等进行采集汇聚。
      4. 安全分析：在采集汇聚的数据基础上，将大量线索进行串接，由点及面进而发掘恶意行为；从威胁的角度出发，建立安全行为基线，实现对异常行为、异常流量进行有效监控；最后可通过算法模型和安全事件结合对攻击的发生概率、损失等进行分析。

#### 威胁主动诱捕

结合蜜罐、大数据等平台对攻击者攻击行为进行识别、跟踪等主动干预，以达到威胁主动诱捕的效果。通过干扰攻击者的认知，隐匿真实数据资产，扭转攻防不对称局面。

#### 恶意程序分析服务

##### 服务内容

协助客户分析恶意程序的特征，以便后续开展针对性防控。

在服务期内，xxxx公司将根据客户的要求，分析客户通过邮件等新式发送的恶意程序样本，分析内容包括但不限于其恶意行为特征、包含的手机号码、邮箱等不法分子信息，并提供针对性的防控建议。

分析报告应在客户发送样本后的2个工作日内完成并反馈客户。

##### 服务方法

1、分析总结

（1）主要观察结果

（2）建议

（3）限制

（4）报告日期和作者

2、分类

（1）文件名

（2）文件大小

（3）文件类型

（4）散列文件

（5）识别的杀毒软件

3、特性

（1）感染的能力

（2）自我保护的能力。

（3）扩散机制

（4）数据泄漏能力

（5）远程攻击者的迭代

4、依赖关系

（1）支持操作系统

（2）所需的Libs

（3）配置文件

（4）脚本和可执行文件

（5）URL的

5、代码分析和行为

（1）行为分析

（2）静态代码分析

（3）动态代码分析

（4）内存的分析

6、支持元素

（1）日志

（2）截图

（3）函数列表

（4）字符串

7、事件的建议

（1）IOC

（2）消除步骤

##### 成果输出

恶意程序样本分析报告。

### 应急响应

#### 服务内容

在服务期内，当客户信息系统遇到突发的安全问题如：发生网络入侵事件、大规模病毒爆发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决时，在收到客户及相关单位的应急响应服务请求信息后，xxxx公司应急小组根据需求，以远程或现场的方式协助客户及相关人员查明安全事件原因，确定安全事件的威胁和破坏的严重程度。并根据对事件的分析及原因提供相应的解决方案。必要时，xxxx公司将配合第三方安全服务机构进行安全应急响应服务。

具体服务内容如下：

安全事件响应分析：在系统出现系统恶意入侵、恶意资源消耗、病毒爆发及其他各类安全事件时，xxxx公司应在规定的安全应急响应时间内，派出应急响应人员对安全事件进行分析和处理。

安全灾难恢复：当系统由于出现安全事故，造成系统无法正常对外提供服务时，xxxx公司应在服务要求中规定的安全应急响应时间内，派出应急响应人员协助客户完成包括但不限于：系统安全恢复，应用服务安全恢复，数据安全恢复，网络性能安全恢复，网络病毒灾难恢复等在内的灾难恢复工作。

安全事件入侵追踪和取证：在系统出现各类型安全事件后，xxxx公司负责对安全事件进行分析，开展安全事件入侵追踪和取证、犯罪取证、事后安全分析和处置服务。

#### 服务流程



应急响应服务事件处理流程主要分为三个阶段，包括事件初期、应急响应实施及输出报告与汇报：

* 事件初期

在实施应急响应工作前，项目经理收到客户或相关网站应急响应服务需求后，由项目经理协调内部应急响应人员和客户相关技术人员第一时间取得联系，了解事件发生情况。应急响应人员判断事件类型，是否需要启用应急响应服务。

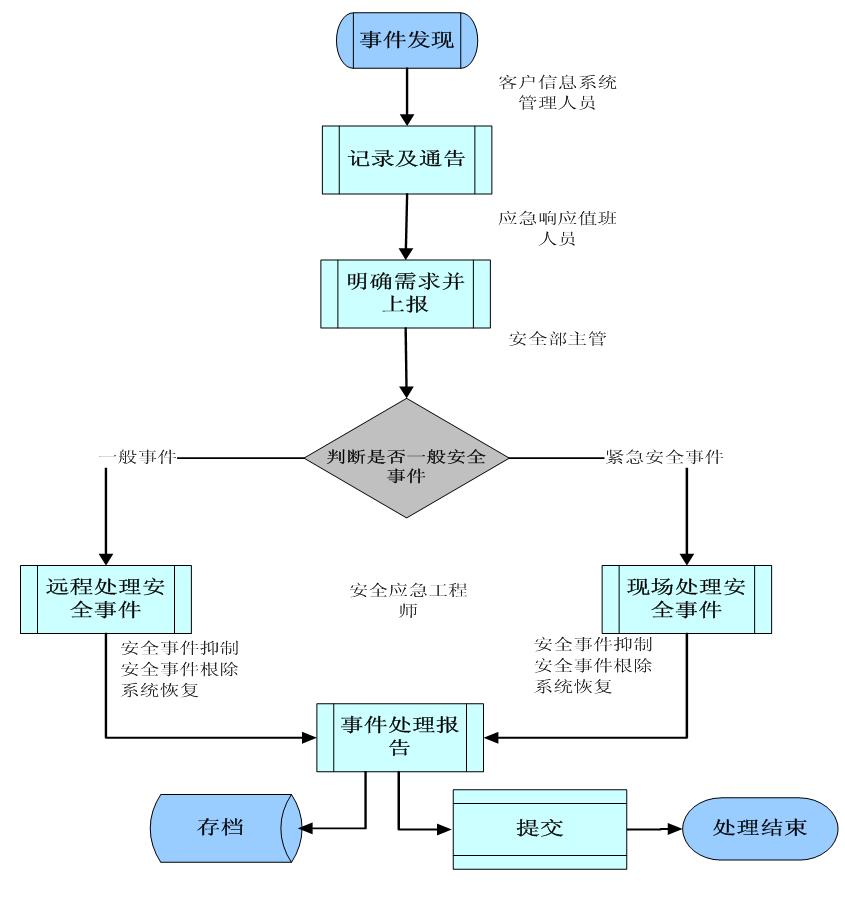
* 应急响应实施

在判断事件类型可能为安全事件，启用应急响应后，应急响应人员通过现场或非现场等方式进行信息收集工作，详细了解掌握事件发生的始终、现状、可能的影响，对事件进行详细分析，提供事件处理建议，并协助客户或相关单位解决事件。

* 输出报告与汇报

待事件处理结束后，应急响应人员整理事件分析、事件处理的过程记录和相关资料，撰写应急响应服务记录报告，提交给客户或相关单位。对于大型、复杂的应急响应过程还需进行整体的事件处理汇报工作。

##### xxxx公司应急流程



图：应急响应流程

#### 服务方式

现场服务：监测小组发现有恶意攻击并需要应急响应时，会在客户现场协助客户分析事件可能的原因，解决各类安全事件。

xxxx公司可提供7×24小时远程（电话、网络等）支持和按需现场应急响应技术支持服务，问题处理完毕后24小时内提供问题分析及处理报告。

#### 服务工具

xxxx公司自主研发的应急响应工具箱。

#### 工作计划

xxxx公司应急小组成员按照“事中监测、事后处置”的原则开展工作。

事中监测阶段：xxxx公司应急小组针对客户系统进行7x24小时监测，一旦发生应急事件，立即按照本预案中规定的流程及时上报并处置。

事后处置阶段：接到应急事件处置指令，应急小组成员迅速行动。第一步：按照应急预案，采取紧急措施，尽可能地降低和避免事件造成的影响，恢复系统正常运行，并将有关情况迅速通告客户；第二步：分析造成安全事件的根源；第三步：总结发生安全事件的原因，及时上报客户，并输出过程文档及完整的信息安全事件应急处置报告。

#### 事件分级及响应说明

xxxx公司根据应急情况出现的严重程度、影响范围、处置时间长短和实施应急方案时所需调动的资源，将服务故障分为三个等级：

|  |  |  |
| --- | --- | --- |
| 严重程度 | 影响范围 | 响应资源 |
| 轻微故障 | 轻微影响系统使用的故障。 | 安全工程师 |
| 一般故障 | 服务可运行，但非重要功能的使用受限。 | 高级安全工程师 |
| 严重故障 | 服务无法运行或基本无法运行或服务重要功能失效或基本失效。 | 高级安全工程师  安全专家 |

#### 应急预案

##### 入侵系统攻击安全事件

###### 事件类型确定

一般情况，入侵系统攻击安全事件具有以下特征：

* 系统性能严重下降，有不明的进程运行并占用大量的CPU处理时间；
* 在系统日志中发现非法登录者；
* 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；
* 入侵检测系统有相关安全事件报警。

###### 事件处理

入侵系统攻击按照不同的攻击目的，又可分为：以炫耀技术目的的系统入侵恢复，以得到或损坏系统中机密数据为目的的系统入侵恢复，以破坏系统或业务正常运行为目的的系统入侵恢复。不同攻击目的的行为会对系统有不同的影响。根据以上攻击目的，安全事件现场处理有以下三种处理方式：

1. 以炫耀技术目的的系统入侵恢复

有一部分攻击者入侵系统的目的，只是为了向同行或其他人炫耀其高超的网络技术，或者是为了实验某个系统漏洞而进行的系统入侵活动。对于这类系统入侵事件，攻击者一般会在被入侵的系统中留下一些证据来证明他已经成功入侵了这个系统。通常这种类型的系统入侵再细分为以控制系统为目的的系统入侵和修改服务内容为目的的系统入侵。对于这种类型的入侵系统攻击，我们应采取以下应急措施：

1. 记录恢复过程中所有的步骤；
2. 建立被入侵系统当前完整系统快照，或只保存被修改部分的快照，以便事后分析和留作证据；
3. 立即通过备份恢复被修改的系统或者网页；
4. 查看系统目前的网络连接情况，如果发现不正常的网络连接，应当立即断开与它的连接。然后通过查看系统进程、服务和分析系统日志文件，来检查系统攻击者在系统中还做了什么样的操作，以便做相应的恢复；
5. 通过分析系统日志文件，或者通过弱点检测工具来了解攻击者入侵系统所利用的漏洞，并升级补丁弥补漏洞；
6. 修复系统或应用程序漏洞后，还应当添加相应的防火墙规则来防止此类事件的再次发生，并升级系统中IPS和杀毒软件的特征库；
7. 最后，使用系统或相应的应用程序检测软件对系统或服务进行一次彻底的弱点检测，在检测之前要确保其检测特征库是最新的，并根据弱点检测结果进行相应的安全加固。所有工作完成后，还应当在后续的一段时间内，安排专人对此系统进行实时监控，以确信系统已经不会再次被此类入侵事件攻击。

* 以得到或损坏系统中机密数据为目的的系统入侵恢复

目前，大部分攻击者都是以获取企业中机密数据为目的而进行的相应系统入侵活动，以便能够通过出售这些盗取的机密数据来获取非法利益。这类攻击行为会造成数据泄密或者数据破坏，因此应急处理的首要任务就是保护内部数据的安全。对于这种类型的入侵系统攻击，我们应采取以下应急措施：

1. 立即找到与攻击源的网络连接并断开，然后通过添加防火墙规则来阻止；
2. 建立被入侵系统当前完整系统快照，或只保存被修改部分的快照，以便事后分析和留作证据；
3. 立即通过备份恢复被修改的系统；
4. 查看系统目前的网络连接情况，如果发现不正常的网络连接，应当立即断开与它的连接。然后通过查看系统进程、服务和分析系统和服务的日志文件，来检查系统攻击者在系统中还做了什么样的操作，以便做相应的恢复；
5. 修改数据库管理员帐号名称和登录密码，重新为操作数据的用户建立新的帐户和密码，并且修改数据库的访问规则；
6. 通过分析系统日志文件，或者通过弱点检测工具来了解攻击者入侵系统所利用的漏洞，并升级补丁弥补漏洞；
7. 修复系统或应用程序漏洞后，还应当添加相应的防火墙规则来防止此类事件的再次发生，并升级系统中IPS和杀毒软件的特征库；
8. 最后，使用系统或相应的应用程序检测软件对系统或服务进行一次彻底的弱点检测，在检测之前要确保其检测特征库是最新的，并根据弱点检测结果进行相应的安全加固。所有工作完成后，还应当在后续的一段时间内，安排专人对此系统进行实时监控，以确信系统已经不会再次被此类入侵事件攻击。
9. 以破坏系统或业务正常运行为目的的系统入侵恢复

攻击者入侵系统的目的，就是为了让系统或系统中的业务不能正常运行，如果我们发现不及时，当这类系统入侵事件攻击成功后，就会造成系统意外停机事件和业务意外中断事件。处理这类系统入侵事件时，已经没有必需再考虑系统需不需要停机处理的问题了，既然系统都已经不能正常运行了，考虑这些都是多余的，最紧要的就是尽快恢复系统正常运行，尽量加快系统和业务恢复正常运行的速度，减少它们停止运行的时间，尽量降低由于系统停机或业务中断造成的影响和损失。对于这种类型的入侵系统攻击，我们应采取以下应急措施：

1. 立即找到与攻击源的网络连接并断开，然后通过添加防火墙规则来阻止；
2. 建立被入侵系统当前完整系统快照，或只保存被修改部分的快照，以便事后分析和留作证据；
3. 立即通过备份恢复被修改的系统；
4. 在系统中重新安装与业务相关应用程序，并且尽量通过备份恢复与业务相关的数据；
5. 查看系统目前的网络连接情况，如果发现不正常的网络连接，应当立即断开与它的连接。然后通过查看系统进程、服务和分析系统和服务的日志文件，来检查系统攻击者在系统中还做了什么样的操作，以便做相应的恢复；
6. 修改数据库管理员帐号名称和登录密码，重新为操作数据的用户建立新的帐户和密码，并且修改数据库的访问规则；
7. 通过分析系统日志文件，或者通过弱点检测工具来了解攻击者入侵系统所利用的漏洞，并升级补丁弥补漏洞；
8. 修复系统或应用程序漏洞后，还应当添加相应的防火墙规则来防止此类事件的再次发生，并升级系统中IPS和杀毒软件的特征库；
9. 使用系统或相应的应用程序检测软件对系统或服务进行一次彻底的弱点检测，在检测之前要确保其检测特征库是最新的，并根据弱点检测结果进行相应的安全加固。所有工作完成后，还应当在后续的一段时间内，安排专人对此系统进行实时监控，以确信系统已经不会再次被此类入侵事件攻击。

##### 拒绝服务攻击安全事件

###### 事件类型确定

一般情况，拒绝服务攻击安全事件具有以下特征：

* 拒绝服务，正常用户不能访问服务器提供的相关服务；
* 系统性能严重下降，有不明的进程运行并占用大量的CPU处理时间；
* 网络流量突发增长，并导致网络延时加大；
* 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；
* 入侵检测系统有相关安全事件报警。

###### 事件处理

拒绝服务攻击按照不同的攻击模式，又可分为：

* SYN Flood攻击；
* IP欺骗DOS攻击；
* UPD洪水攻击；
* PING洪流攻击；
* 泪滴攻击；
* Land攻击；
* Smurt攻击；
* Fraggle攻击。

不管是何种拒绝服务攻击，最终目的都是造成网络资源或者主机资源的耗尽，因此，针对拒绝服务攻击，应采取以下应急响应处理措施：

* 记录恢复过程中所有的步骤；
* 立即启动应付策略，尽可能快的向回追踪攻击包的来源；
* 利用边界路由器的Guard防DDos攻击模块，进行拒绝服务攻击流量牵引；
* 联系电信运营商，协助实现路由的访问控制，以实现对带宽总量的限制以及不同的访问地址在同一时间对带宽的占有率，并通知运营商终止攻击包的源地址的连接；
* 减少对外服务，更改路由器配置，增加包过滤策略，尽量使对外服务最小化，减少对外连接数，减轻带宽压力；
* 对遭受攻击的主机也要同样进行设置保护，在服务器上关闭端口，禁止一切不必要的服务；
* 如果可能，可以断开网络与主机的网络连接，以便于在非联机状态下恢复系统，并更新升级系统补丁。

##### 病毒与木马攻击安全事件

###### 事件类型确定

一般情况，病毒与木马攻击安全事件具有以下特征：

* 防病毒软件发出病毒警告；
* 系统性能严重下降，有不明的进程运行并占用大量的CPU处理时间；
* 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；
* 有不明的对外网络连接；
* 文件的访问权限被修改；
* 因安全漏洞导致的系统问题；
* 入侵检测系统有相关安全事件报警。

###### 事件处理

针对病毒与木马攻击，应采取以下应急响应处理措施：

* 记录恢复过程中所有的步骤；
* 发现病毒或者接到病毒报告后，马上断开染毒的计算机的网络连接，升级病毒防护系统至最新病毒库，并对染毒的计算机和网络进行病毒检查；
* 检查其他机器是否染毒，并采取措施杀毒；
* 立即准备好备用机器，并做好配置；
* 替换染毒的计算机；
* 系统恢复对外；
* 对染毒的计算机进行杀毒；
* 登记本次病毒情况；
* 如果事件扩大，病毒传播严重，需要报告“xxxx公司信息”安全专家，由安全专家到场进行杀毒和隔离等措施的处理，必要时候，可以启用备份和恢复策略进行恢复。

##### 网站页面篡改安全事件

###### 事件类型确定

一般情况，网站页面篡改安全事件具有以下特征：

* 网站内容被更改；
* 网站被挂马；
* 网站链接被篡改；
* 入侵检测系统有相关安全事件报警。

###### 事件处理

针对网站页面篡改安全事件，应采取以下应急响应处理措施：

* 记录恢复过程中所有的步骤；
* 确认网页被篡改严重程度，如果网页被挂马或者影响恶劣，立即关闭被篡改网站服务器，然后通知安全厂商进行排查；
* 确认被篡改网页所在的服务器，使用网站系统备份恢复网站内容；
* 查找被篡改网页所在的服务器的漏洞，恢复网页，并修复漏洞，删除入侵者留下的可用资源；
* 必要情况下（如网页被篡改内容包含法轮功、藏独等政治性信息），建议立即关闭信息系统服务器，并通知相关部门（当地公安网络信息安全监查大队）。

##### 数据库内部误操作

###### 事件类型确定

一般情况，数据库内部误操作安全事件具有以下特征：

* 数据库用户登录异常；
* 数据库配置异常更改；
* 数据库重要数据被异常删除；
* 数据库审计系统有相关安全事件报警；
* 其它的误操作行为。

###### 事件处理

针对数据库内部误操作安全事件，应采取以下应急响应处理措施：

* 记录恢复过程中所有的步骤；
* 确认数据库误操作严重程度，使用数据库系统备份恢复数据内容；
* 必要情况下（数据库系统发生严重错误或内容严重缺失），建议立即关闭数据库系统服务器，并通知相关部门（当地公安网络信息安全监查大队）。

#### 成果输出

xxxx公司根据每次安全应急响应的情况，提交《应急响应报告》。

### 威胁情报

#### 服务内容

根据目前的信息安全形势，xxxx公司定期向客户中心提供互联网安全威胁态势通报动态，涉及客户信息安全的高危漏洞进行准确快速的分析及安全预警。包括但不限于操作系统、数据库、中间件等基础软件、应用软件、硬件设备、工具软件等，每周发送分析和预警报告。

在发生重大安全事件或有相关安全漏洞信息发布时，直接通过电话或短信为客户中心网站安全管理人员提供相关的信息通告。

在权威部门（公安部、人民银行、银保监会、CNCERT等）发布高危漏洞信息2日内，提交漏洞预警报告。

具体通告内容如下：

1. 互联网最新病毒及其解决方法信息：将最具威胁性的病毒信息编制成册，包括病毒危害、感染原理及防护措施等；
2. 互联网最新系统漏洞信息及其修补方法：将各操作系统、应用系统、网络设备等最新安全漏洞编制成册，包括漏洞威胁、影响平台及修补方法等；
3. 互联网最新攻击方式信息以及防御措施：一旦出现将可能造成大规模网络攻击事件的安全漏洞或病毒木马，及时通知相关人员进行安全预警，积极进行补丁修复和安全防护工作；
4. 互联网最新发生的安全事件：将相关信息安全事件编制成册，避免信息系统遭遇同样安全攻击，造成严重损失；

#### 服务流程

xxxx公司首先进行信息收集、汇总分析，制定固定的互联网安全态势模版，一般互联网安全态势通告通过Email告知，并对可能系统产生影响的风险，出具相应的解决方案。

#### 服务方式

xxxx公司将采取： Email方式来进行互联网安全威胁态势通告。

#### 成果输出

xxxx公司定期发送《互联网威胁情报通告》，报告中包含漏洞介绍、危害程度、影响范围、处置措施等内容。

## 重保总结服务

### 复盘总结服务

在全年重保活动结束后，xxxx公司将对整个过程发现的安全漏洞以及攻击手段等内容进行全方面的总结。并根据需要，对安全漏洞进行全面分析并形成整改报告，督促各部门整改及上报整改结果。

在此阶段，xxxx公司可为客户提供以下服务：

重保活动结束，协助客户进行整改。并分析漏洞信息，总结保障情况，进行培训。进一步提升客户内部人员的技术水平，提高网络安全防护水平，提出增强防护建议并落实，建立和完善后续重保活动保障方案。

高级安全专家通过本次事后总结，将漏洞情况、流程、技术以及人员进行全方面的优化整改，完善防护产品及策略、漏洞全流程修复、管理制度完善等。

### 安全优化整改服务

##### 协助整改

在重保活动结束后，客户组织安全团队对重保活动过程发现的安全漏洞，结合威胁情报和本地的攻击日志。并根据需要，可以对入侵的行为进行分析研判和溯源，形成整改报告，并下发到各业务部门，协助其整改及上报整改结果。

xxxx公司可根据在重保活动中发现的安全问题进行协助整改，及时修复已知的安全漏洞。

##### 总结报告

重保活动之后，xxxx公司将向客户提供一份重保活动总结报告，报告十分详细的说明重保活动过程中的得到的数据和信息，并且将会详细的纪录整个重保活动的全部操作。

总结报告应包含如下内容：

测试结论：包括系统的安全状况、存在的问题、重保活动的结果等。

真实攻击的证据：真实攻击的一些过程及证明文件。

针对重保活动中发现的问题给出对应的解决办法和防护建议。