网络安全应急演练方案

1. 网络安全应急演练方案
2. 指导思想

根据《中华人民共和国网络安全法》规定，定期开展安全应急演练工作，网络实战网络安全应急演练便是在新的网络安全形势下，通过攻防双方之间的对抗演习，实现“防患于未然”。

1. 演练目的

通过网络实战网络安全应急演练，检验并完善移动关键基础设施网络安全应急响应机制与提高技术防护能力，检验各公司遭遇网络攻击时发现和协同处置安全风险的能力，培养和提升网络安全人才实战能力，全力保障建党 100 周年大庆等国家重大活动网络安全。

1. 演练时间

演练时间：2023 年x 月x 日

1. 演练内容

网络与信息安全事件应急演练

1. 演练流程

网络安全应急演练保障活动共分为启动阶段、准备阶段、演练阶段、保障阶段、总结阶段五个阶段，具体工作安排计划如下：

启动阶段：确定演练目标、人员团队职责划分、演练总体流程，后续工作提供指导。

准备阶段：需对演练目标进行安全分析和梳理，开展全面安全评估、关注现有安全能力、完成安全策略的全面优化人员的全面赋能等。

演练阶段：重点检测演练系统的监测手段和防御手段的有效性及安全人员操作规程熟悉度。

保障阶段：为保障业务系统的平稳运行，避免因安全问题而导致出现重大事故。

总结阶段：对行动中发现的相关问题进行快速整改并进行总结，将经验固化至相关的规章制度中，形成常态化、制度化。

1. 演练方案
   1. 启动阶段
      1. 演练组织及职责分工

在网络安全应急演练保障期间，组织建立保障小组，通过签署责任书，明确保障人员职责，确保各司其职，有序开展保障工作。

**总指挥**

* 负责网络安全应急演练保障期间重大决策；
* 把控项目的整体进度及质量；

**指挥决策组**

* 协调各小组资源分配，起到上传下达的等作用；
* 演习保障结束后，负责对演习保障进行总结，形成报告并输出安全能力建设的规划；
* 协同其他各小组完成安全事件的闭环；

**安全监控小组**

* 通过实时监控平台、或设备日志，发现网络中的异常流量、恶意样本、网络攻击行为；
* 发现异常行为后，按事件模版及时将攻击事件通报；

**分析研判小组**

* 通过对主机日志、网络设备日志、安全设备日志以及全流量分析等信息对攻击行为进行分析，找到攻击者的源 IP地址、攻击服务器 IP 地址、邮件地址等信息；

**应急处置小组**

* 恢复系统备份、数据恢复等方式将系统业务恢复到正常

状态；

* 将完整的应急处置、溯源流程记录到报告，并上报给保障决策组；

**支撑小组**

* 支撑小组为二线专家小组，协助现场一线工作小组解决并提供专业安全业务建议。
  + 1. 演练保密要求

在网络安全应急演习保障期间，开展参演人员安全意识宣贯、签订网络安全承诺书和安全保密协议。宣贯内容包含但不限于：代码管理规范、接入账号安全、接入网络安全、办公设备安全等。

网络安全承诺书内容至少包含但不限于：遵守甲方整体网络安全工作要求、遵守相关法律及行业相关规定、强化项目参与人员的信息安全意识、违约责任等。

保密协议内容至少包含但不限于：演习保障期间的保密范围、保密期限、保密要求、违约责任等。

* 1. 准备阶段
     1. 信息资产收集

在网络安全应急演练准备阶段，对演练系统进行信息收集包括单不限于 IP 地址、端口、服务名称及版本、操作系统类型及版本、应用框架类型及版本等，为开展演练行为做基础。

在网络安全应急演练保障实施期间，信息资产收集可助于快速发现内部问题、定位问题、解决问题，提高企业内部的防御能力。

* + 1. 全面安全评估

对演练系统涉及的主机、数据库、应用组件、网络设备、网络架构进行全面、综合的安全评估，充分的发现其潜在的风险。

* + 1. 安全策略优化

根据网络安全架构评估以及网络现状，对网络设备策略、安全设备策略、主机策略等进行进一步调整和优化实施范围。

* + 1. 安全缺陷整改

根据之前业务系统评估，对应用系统及其依赖的网络、数据信息等可能存在的软硬件缺陷，和信息安全管理中潜在的薄弱环节，而导致的不同程度的安全风险，提出临时解决方案和长期解决方案。

* + 1. 安全意识培训

在网络安全应急演练备战阶段，为了提升内外部人员的安全意识，组织开展安全意识宣贯和安全技术赋能，避免因人为因素而导致信息安全事件发生，整体提高安全管理能力。

* 1. 演练阶段
     1. 攻防场景演练

采用攻防对抗的方式有效的检验相关业务系统的抗攻击能力，真正发现潜在的风险，从而为后续整改工作提供真实有效的依据。

* + - 1. 攻击方工作
         1. 攻击路径设计

攻击者可以通过各种方式各种攻击路径尝试攻破应用系统去危害客户的业务或者企业组织。每种路径方法都代表了一种风险。结合攻击路径相关的技术和对客户的业务影响评估威胁来源、攻击向量和安全漏洞的可能性。渗透测试设计内容

针对信息系统业务系统和平台进行全局、深入安全渗透测试，关注其面临的主要安全风险和安全需求，提供安全渗透测试数据报告和针对性解决方案，建立一体化信息系统安全风险识别机制。

* + - * 1. 应用功能测试

发现目标系统中存在的安全隐患（包括安全功能设计、安全弱点、以及安全部署中的弱点等），并针对问题提供解决方案建议。

* + - * 1. 安全功能弱点测试

应用系统评估主要从输入验证、身份验证、授权、配置管理、敏感数据保护、会话管理、加密、异常管理等角度分析应用系统的安全功能设计以及存在的安全隐患。

* + - * 1. 应用安全性测试

针对提供的业务系统进行非破坏性的模拟黑客攻击，充分挖掘应用系统各类组件存在的漏洞，并进行人工利用验证。

* + - 1. 防守方工作

在攻防对抗中，通过部署监测预警功能的平台，针对攻击行为进行监控及时阻断并上报，从而形成闭环的处置工作。

在防守监测工作中，需结合现有态势平台、处置平台以及相关设备进行合理利用。

* + - * 1. 设备运行监控

针对安全产品、网络产品、主机服务器等提供监控与运维服务，及时发现设备（系统）运行过程中出现的问题并协助客户进行解决，保障设备（系统）正常运转。

监控指标可涵盖设备功能、设备性能、应用服务情况、连通性、操作审计等。

* + - * 1. 告警事件监控

针对各类安全设备的告警数据进行监控，通过人工告警研

判的方式对安全设备告警进行二次分析，排除告警中的误

报，定位真实风险。

监控告警类型可涵盖：DDoS 攻击、Web 攻击、信息破坏、 口令猜测、僵尸主机、木马病毒、非授权访问、漏洞利用网页篡改、SQL 注入、非法连接、恶意扫描探测、网页篡改、网站敏感内容、网页挂马等。

* + - * 1. 安全事件溯源

防守方对多种网络安全设备产生的丰富的日志和告警信息集中分析，发掘安全知识的效果，发现传统安全工具难以发现的安全事件。通过人工的方式判断安全事件是否为误报后，追溯该告警背后的威胁源，判断威胁源使用的攻击手段及漏洞利用情况。

攻击溯源方案可分为三个层次的追踪：追踪溯源攻击主机追踪溯源攻击控制主机、追踪溯源攻击者和追踪溯源攻击组织机构。

* + - * 1. 安全事件处置

对于安全监控中发现的安全对象脆弱性问题（如高危漏洞

安全基线配置不合格等）、安全故障问题、安全事件等，监控值守人员通过攻防平台提供的工单流程进行处置任务指派，运维人员、二线支持人员及管理人员依照工单流程完成安全处置工作。

* + 1. 应急场景演练

通过模拟攻击者发起 0 day 攻击，对安全监控、安全防护、 网络策略、安全策略等机制进行有效性校验，按照流程快速响应，推动 0day 的缓解处理和后续补丁修复，最大化减少 0day 的影响。对发现问题及时推动整改，闭环安全风险，确保自身的网络策略、安全策略符合安全预期。

安全监控小组负责漏洞信息监测收集和危害判断，发现问题后通知分析研判小组、应急处置小组，通过资产管理平台或相关检测工具，确定受该漏洞影响的资产范围，再按照资产价值（重要程度）和网络暴露情况确定漏洞修复的优先级，确立响应的等级、需要哪些部门（厂商）参与。

做好内部的漏洞修复通知和外部的业务升级暂停公告，应急处置小组协助做好系统备份工作，并且在非业务时间段

实施升级。漏洞修复后，业务归属部门自行检查业务功能

是否受影响，校验数据是否丢失。

0 day 漏洞处理流程示意图如下图所示：

完成 0day 处置的同时，应将其加入安全开发知识库，避免后续发生类似的安全问题。

* + 1. 应急响应支撑

应急响应能够快速成功处置，关键是根据前期应急预设流程为指导，应急处置小组有条不紊对已发生安全事件进行解决，以最大限度地减少安全事件造成的损害，降低应急处置中的风险。

* + - 1. 检测阶段

检测是指以适当的方法确认在系统/网络中是否出现了恶意代码、文件和目录是否被篡改等异常活动/现象。

安全监控小组在检测到网络安全事件或发现信息系统异常上报分析研判小组。

分析研判小组立即对上报事件的性质、影响范围、安全设备日志告警进行分析与评估。

* + - 1. 分析阶段

该阶段确定它的影响范围和问题原因及事件的性质。

分析研判小组通过安全事件告警日志进行分析研判，评估事件的性质、影响范围判断，是否上报应急处置小组，开展应急响应：

若判断无需开展应急响应，发布相关预警通告，应急流程结束；

若判断需开展应急响应，则结合实际情况对网络安全事件进行定位，启用相应的专项应急预案，上报演习保障决策组，并通知应急处置小组开展应急响应。

应急处置小组根据应急预案处置流程开展应急处置操作。

* + - 1. 抑制阶段

恢复阶段是它的目的是限制攻击/破坏所波及的范围。同时也是限制潜在的损失。所有的抑制活动都是建立在能正确检测事件的基础上，抑制活动必须结合检测阶段发现的安全事件的现象、性质、范围等属性，制定并实施正确的抑制策略。

应急处置小组按照应急预案开展应急处置，执行抑制方案并记录抑制过程，检查恢复效果，如果抑制不成功则收集信息重新制定抑制方案。

在此阶段，保障决策组协调资源进行技术或业务支撑，必要时协调支撑小组进行支撑，协助开展事件处置、业务恢复、系统监控等工作内容

* + - 1. 根除阶段

根除阶段即在准确的抑制事件后，找出事件的根源并彻底根除它，以避免攻击者再次使用相同手段攻击系统，引发安全事件。在根除阶段中将需要利用到在准备阶段中产生的结果。

应急小组按照应急预案对关键业务信息执行备份和状态检

查，对事件进行原因分析，对业务系统进一步进行检查，根据发现的问题与漏洞制定事件根除方案。

在此阶段，支撑小组协调资源协助应急小组开展业务系统排查、漏洞整改等工作内容。

* + - 1. 恢复阶段

应急小组按照应急预案开展应急处置和业务恢复工作，由应急执行小组组织相关部门安全管理员和运维操作人员等技术人员对网络安全事件进行现场处置，执行恢复方案，并记录恢复过程，检查恢复效果，如果恢复不成功则收集信息重新制定业务恢复方案，尽快恢复系统正常运行。

系统恢复后及时将事件处置结果逐级上报至集团应急领导小组。

* + - 1. 总结阶段

该阶段的目标是回顾并整合发生事件的相关信息，主要有助于从安全事件中吸取经验教训，提高技能；有助于评判

应急响应组织的事件响应能力。

应急处置小组对业务影响、范围、损失进行总结，对应急措施的有效性进行评估，对事件原因进行分析，编写安全事件处置总结报告。

应急处置小组向指挥决策组提交报告，并组织各业务系统管理人员对类似安全隐患的业务系统进行自查自检，必要时可采取紧急抑制手段避免同类安全事件的发生。

* 1. 保障阶段

在演习实战阶段，为保障业务系统的平稳运行，避免因安全问题而导致出现重大事故，将开展安全值守监控、配合中台支撑的优势，研判预警通告、威胁分析、应急响应支撑及演习事件上报等工作。

* + 1. 安全值守监控
       1. 网站及业务监控

1. 主机资产监控

在演习保障期间，为及时发现资产对外暴露安全风险，安全监控小组将定时对外网资产进行监测，统计当天外网活跃主机数目，开放端口个数及端口服务类型，并通过人工分析确认是否存在异常端口对外开放。

1. 网站安全监控

在演习保障期间，对网站提供完整性检测、可用性检测。完整性监测能够甄别出防护站点页面是否发生了恶意篡改是否被恶意挂马，是否被嵌入敏感内容等信息；可用性检测能够帮助防守方了解站点此时的通断状况，延迟状况。

* 1. 远程网页挂马及黑链监测：远程实时监测目标站点是否存在被植入恶意代码、黄赌毒私服等词汇的恶意链接的告警在第一时间得知在防护网站的安全状态，及时清除网页木马及黑链。
  2. 远程网页篡改监测：远程实时监测目标站点是否是存在页面被篡改情况，避免网站被篡改不能及时发现，造成恶劣影响，此服务是网站防护的最后一道屏障。
  3. 远程网站域名监测：实时监测各地主流 ISP 的 DNS 缓存服务器和客户 DNS 授权服务器的可用性，以及它们对被监测域名的解析结果情况。一旦发现客户域名无法解析或解析不正确，第一时间上报评估小组进行处置。
  4. 远程网站平稳度监测服务：远程实时监测目标站点在多种网络协议下的响应速度、首页加载时间等反映网站性能状况的内容，一旦发现客户域名无法解析或解析不正确，第一时间上报评估小组进行处置。
     + 1. 安全设备监控

在网络安全应急演练保障期间，安全监控小组对安全设备进行监控，开展设备性能监控、安全攻击监控等工作。

a)安全攻击监控：安全设备告警事件实时监控，包含：拒绝服务攻击，网络病毒爆发，漏洞远程利用、恶意代码传递等高危事件告警信息，对攻击告警日志进行分析处置，策略调整优化，对高危风险行为 IP 执行封禁封堵，可密切关注来源请求异常，接口请求异常，恶意 IP 攻击等事件。

* + - 1. 安全行为监控

在网络安全应急演练实战期间，VPN、堡垒机、关键设备主机等设备是黑客突破的重要目标，当获取到权限账户后，黑客可能会选择在夜间薄弱时间点发起攻击行为，或执行高危操作，故安全监控小组将对设备账户安全行为进行监控，并对日志进行安全审计。

安全监控小组通过人工分析日志，审计目前监控设备是否存在僵尸账户、异地登录、频繁登录、异常时间登陆、账户威胁操作等行为情况，并针对不同事件采取相应措施，防止风险扩散。

1. 僵尸账户分析：安全监控小组通过人工分析日志，查找近期未活跃的账户，对疑是僵尸账户进行逐一确认，非必要账户或权限不合理账户，需进行回收处理。
2. 异地登录分析：安全监控小组通过人工分析日志，查看设备账户近期是否频繁更换登陆地点，地点变更间隔是否符合常理，对出现异常账户进行逐一确认，确保账户登录环境安全。
3. 频繁登录分析：安全监控小组通过人工分析日志，查看设备账户近期是否存在频繁登录行为，重点关注频繁登录失败事件，分析当前账户是否遭受暴力破解。
4. 异常时间登录分析：安全监控小组通过人工分析日志，查看设备账户近期是否在异常时间段(凌晨 1 点至 6 点)期间登录，对出现异常账户进行逐一确认，确保账户均为账户申请人本人操作。
5. 账户威胁操作分析：安全监控小组通过人工分析日志，查看设备账户近期执行是否正常，如删除数据库、修改关键信息等操作，对出现异常账户进行逐个确认，确保高风险操作是正常操作。
   * + 1. 重要系统巡检

系统巡检工作能保证服务器正常、有序、安全地运转，保障更好地应用网络及相关服务。在网络安全应急演练实战期间，靶标、关键系统、服务器等设备是突破的重要目标通过对重要系统的巡检，可发现目标存在的一些异常，以便在系统故障或应急事件发生时及时作出处理，减少不良影响。系统可用性检查检查设备或服务器系统时间、是否升级包、证书信息等信息。

1. 系统日志分析

通过对日志进行统计、分析、汇总，能有效掌握服务器的运行状况，及时发现问题，排除安全隐患。其中关注以下几个方面的行为日志：

* 1. 可疑账户的登录：查找登录的账户，对可疑账户进行逐一

确认、非必要账户、权限不合理账户，进行回收处理。

* 1. 异地登录的账户：查看设备账户近期是否频繁更换登陆地点，地点变更间隔是否符合常理，对出现异地账 户进行逐一确认，确保账户登录环境安全。
  2. 频繁登录分析：查看设备账户是否存在频繁登录行为，重点关注频繁登录失败事件，分析当前账户是否遭受暴力破解。异常时间登录分析：查看设备账户近期是否在异常时间段(非工作时间段)期间登录，对出现异常账户进行逐一确认，确保账户均为账户申请人本人操作。
     + 1. 重要设备监控

在网络安全应急演练实战期间，安全监控小组对安全设备进行监控，开展设备性能监控、安全攻击监控等工作。

1. 设备性能监控

安全设备健康情况实时监控，包含：CPU 使用率、内存占用率、接口流量、接口工作状态、硬盘使用情况等设备健康相关的基本参数监控，监控过程需密切关注设备性能占比通过分析当前业务负载，及设备各项性能指标，确保过程中设备可用性。

1. 系统性能检查

检查服务器资源使用情况，合理分配资源，能够提高服务器的工作效率。内存不足或 CPU 使用率居高不下，不仅对服务器性能造成较大影响，而且可能存在攻击或病毒感染等问题。通过对磁盘剩余空间、CPU、进程、内存等参数进行检查，掌握系统目前的运行状况。

1. 数据备份检查

查数据备份是否存在或异常的情况，能为之后可能出现的系统故障处理提供保障。方便故障后恢复系统配置提供极大的便利。

* + 1. 研判预警处置

在网络安全应急演练保障期间，研判分析小组将对安全监控小组上报事件进行研判处置，对符合预警条件的事件进行通知处理。

安全预警通告主要类型包括安全风险预警通告、安全事件应急通告、可疑安全行为通告，当研判分析小组收到上述通告时，及时研判被通告事件与保障目标资产吻合度，对风险内容进行定位分析，确认实际影响范围，威胁程度，紧急程度等，并协调应急处置小组进行处理，以达到快速闭环安全风险目的。

1. 安全通告接收

安全监控小组接收到安全风险预警，安全事件应急及可疑安全行为等各类安全事件。

1. 安全通告研判

研判分析小组研判被通告事件与保障目标资产吻合度，对风险内容进行定位分析，确认实际影响范围，威胁程度，紧急程度等。

1. 安全通告处置

协调应急处置小组对安全风险进行闭环，并记录进统计表中。

* + 1. 安全事件上报

在网络安全应急演练保障期间，防守方对检测到的告警信息进行研判分析，对确属攻击行为的安全事件，及时根据规定格式编写防守方成果报告，提交至保障决策组，由安全接口人统一上报。

* + 1. 安全事件跟踪

将针对网络安全应急演练前期的待处理事件和中期发生的安全事件进行梳理，根据安全问题风险程度由高到低设置处理优先级，绘制输出安全事件跟踪表。

* 1. 总结阶段

在网络安全应急演练保障结束后，将对保障期间所涉及到的攻击事件进行汇总梳理，通过分析还原攻击手段，对存在安全缺陷进行整改跟进，总结经验教训，提升业务安全防护能力，强化业务安全。

* + 1. 安全事件梳理

在保障结束后，将组织保障参与人员对应急演练期间出现的攻击事件进行汇总统计，包括但不限于：

针对攻击事件进行攻击时段、频率、次数的统计，分析常

见攻击事件行为识别已受攻击的业务风险；

分析攻击源地址的地域、攻击时间、攻击次数等维度识别攻击者攻击意图；分析攻击目的地址识别易受攻击的业务模块；

从风险等级由高到低排序，重点关注高危行为，根据高危

行为指向的目的地址，识别易受攻击的业务模块。

* + 1. 事件总结归档

在保障结束后，将组织演习保障参与人员进行总结分析，并于收尾会议后的 3 个工作日内，输出网络安全应急演练活动总结报告，并递交至演习保障组、总指挥进行初步审阅及最终审阅，最后发送给保障联络组各小组部门负责人，归档至信息安全部门。

1. 演练平台说明

在网络安全应急演练保障期间，演习保障人员均通过“安全设备—态势感知—攻防平台—封堵平台”形成安全事件从发现、分析、研判、封堵的全生命周期闭环管理。

在演练期间，态势平台会获取所有安全设备事件日志统一处理，攻防平台获取态势平台的安全事件，并前往封堵平

台查看告警 IP 是否被封禁。这一系列动作可通过自动化的

脚本执行，演练人员需要重点查看安全事件是否正常。

1、登录签到

访问攻防平台输入账户、密码进行登陆。若提示证书错误请添加例外或继续访问。登录攻防平台后请先进行签到，点击右上角的日历图标，在我的签到页面下，点击签到。

2、安全设备/事件监控

安全值守监控人员实时监控各安全设备、态势平台、攻防平台、封堵平台的安全事件条数、处置状态，确保各类攻击事件均已处置完毕,对于未处置完毕的安全事件，手工派发安全事件工单，通知对应人员在规定时间内手工处置完毕。

安全值守监控人员实时监控各安全设备（各安全域的DDOS、防病毒、防篡改、WAF、防火墙、天擎、IDS、IPS、态势平台、攻防平台、封堵平台的运行情况，安全值守人员对统计数据进行复核确认。

3、安全事件处置

在攻防平台的左侧进入安全事件中心，查看平台从态势平台所取得的安全事件。点击事件列表右侧的处理，进入事件处理的详情后点击结束事件。此时将事件状态切换为已解决，可以看到刚才的事件状态已经转换成已解决。

在封堵平台的左侧进入攻防封堵页面，查看安全事件处置结果，显示时间处置类型及处置状态。

4、签出

在完成任务后，要点击页面右上角的日历标志，在我的签到页面中，点击签出。