**XXX 单位攻防演习应急预案**

**各类安全事件应急处置手册**

## 扫描事件

### 预案启动条件

经确定是扫描事件后，应当在确认不影响业务系统的前提下，立即启动预案处置工作。

### 预案执行原则

* 系统恢复原则和业务保障原则

对安全事件原因明确的，应按照系统恢复最快为原则。对于不明原因的安全事件，以对业务保障最有力为原则。

### 预案处置工作

**事件诊断确定**

扫描事件具有以下特征：单个或多个IP在一定时间段内，大量的有规律的对系统发起请求。

**事件现场处理**

扫描是攻击的前奏，攻击者通过扫描获取系统。为了防止系统信息泄露，我们应采取以下应急措施：

1. 快速识别扫描源。扫描源可以通过态势感知平台或者系统日志进行查看。碰到扫描事件，需要尽快识别梳理扫描IP。
2. 封堵IP或者IP段。由网络小组对扫描IP进行封堵，加入黑名单。一般建议封堵单个IP；但是如果IP较多，可以封堵IP段，之后再进行详细梳理扫描源。

**事件处置分析**

事件现场处置工作结束后，安全保障工作小组形成《扫描事件应急处置报告》，并由安全保障工作小组组长向安全保障领导小组汇报。《扫描事件应急处置报告》报告内容包括事件处置命令的下达时间、事件处置工作开展时间和结束时间、事件处置人员、事件类型、事件风险分析、事件处置方法、事件处置结果、事件处置建议等方面内容。

## 漏洞入侵事件

### 预案启动条件

经确定是漏洞入侵攻击事件后，漏洞攻击应急专项预案启动应上报安全保障领导小组，安全保障领导小组下达漏洞攻击应急专项预案启动命令后，方可启动和执行漏洞攻击应急专项预案。

### 预案执行原则

* 系统恢复原则和业务保障原则

对安全事件原因明确的，应按照系统恢复最快为原则。对于不明原因的安全事件，以对业务保障最有力为原则。

* 及时通报原则

安全事件处置过程中要将业务影响情况及时上报领导。

### 预案处置工作

**事件诊断确定**

一般情况，漏洞攻击安全事件具有以下特征：

入侵检测系统发现漏洞攻击行为、操作行为；

审计系统记录了漏洞攻击的操作过程；

在系统日志中发现非法登录、操作行为；

入侵行为包括执行操作命令、上传恶意程序、各种非常操作等行为；

通过系统漏洞检查发现对应的入侵利用漏洞。

**事件现场处理**

漏洞入侵事件可以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。对于漏洞入侵系统攻击，我们通常采取以下应急措施：

1.记录恢复过程中所有的步骤；

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，尤其是备份应用日志和系统日志；

1. 根据可疑文件等异常信息进行排查。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；
2. 依据分析结果，进行处置。清除webshell等残留文件，恢复系统正常运行。

4.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；

5 .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。

**事件处置分析**

事件现场处置工作结束后，安全保障工作小组形成《安全漏洞攻击应急处置报告》，并由安全保障工作小组组长向安全保障领导小组汇报。《安全漏洞攻击应急处置报告》报告内容包括事件处置命令的下达时间、事件处置工作开展时间和结束时间、事件处置人员、事件类型、事件风险分析、事件处置方法、事件处置结果、事件处置建议等方面内容

## 口令破解事件

### 预案启动条件

经确定是口令爆破事件后，应当在确认不影响业务系统的前提下，立即启动预案处置工作，无需上报领导小组，但是需要保留攻击记录。处置记录。

### 预案执行原则

* 系统恢复原则和业务保障原则

对安全事件原因明确的，应按照系统恢复最快为原则。对于不明原因的安全事件，以对业务保障最有力为原则。

### 预案处置工作

**事件诊断确定**

口令爆破是一种窃取用户名和密码的行为，它具有以下特征：

攻击者使用单个用户名在一定时间段内，使用不同的有规律的密码进行登录尝试，或者攻击者使用单个密码在一定时间段内，使用不同的有规律的用户名进行登录尝试。

**事件现场处理**

攻击者通过口令爆破有机会获取系统某个用户的用户名和密码，从而在未被授权的情况下使用授权账号进行登录。轻则泄露用户信息，重则失去系统的控制权限，成为攻击者的跳板。

为了防止口令爆破攻击，我们应采取以下措施：

1. 快速识别爆破源。爆破源可以通过态势感知平台或者系统日志进行查看。碰到爆破事件，需要尽快识别梳理爆破IP。
2. 封堵IP或者IP段。由网络小组对扫描IP进行封堵，加入黑名单。一般建议封堵单个IP；但是如果IP较多，可以封堵IP段，之后再进行详细梳理扫描源。
3. 建议使用强密码。可以使用位数较长、无规律、大小写数字符号混杂的密码。

**事件处置分析**

事件现场处置工作结束后，安全保障工作小组形成《口令爆破事件应急处置报告》，并由安全保障工作小组组长向安全保障领导小组汇报。《口令爆破事件应急处置报告》报告内容包括事件处置命令的下达时间、事件处置工作开展时间和结束时间、事件处置人员、事件类型、事件风险分析、事件处置方法、事件处置结果、事件处置建议等方面内容

## 后门木马事件

### 预案启动条件

经确定是后门木马攻击事件后，后门木马攻击事件应急专项预案启动应上报安全保障领导小组，安全保障领导小组下达后门木马攻击事件专项预案启动命令后，方可启动和执行漏洞攻击后门木马攻击事件应急专项预案。

### 预案执行原则

* 系统恢复原则和业务保障原则

对安全事件原因明确的，应按照系统恢复最快为原则。对于不明原因的安全事件，以对业务保障最有力为原则。

* 及时通报原则

安全事件处置过程中要将业务影响情况及时上报领导。

### 预案处置工作

**事件诊断确定**

一般情况，后门木马攻击事件具有以下特征：

网站被挂马；

态势感知系统感知到后门木马类事件；

态势感知系统感知到异常通信事件；

发现异常进程等。

**事件现场处理**

针对后门木马攻击事件，应采取以下应急响应处理措施：

1. 切断异常的网络连接，请示领导后，可以进行断网操作，处置完成后再上线；
2. 如果攻击者正在实施网页挂马攻击，攻击未成功，则在网络边界防火墙、入侵防御系统、网页防护系统上过滤攻击源地址和操作行为，即封堵攻击IP；
3. 将被攻击的机器脱离网络，线下处理后门木马攻击事件。
4. 手工清除webshell、木马后门、其他恶意程序、图片、文字等内容，并在服务器上安装恶意程序查杀工具进行全面检查。可以根据文件修改时间进行排查清除工作。
5. 通过日志分析事件发生的原因，进行封堵修复。如果是通过漏洞攻击，可使用漏洞工具全面检查服务器漏洞，并更新系统补丁。
6. 对后门木马攻击事件关联机器修复后，进行测试无问题，可重新上线。

**事件处置分析**

事件现场处置工作结束后，安全保障工作小组形成《后门木马攻击事件应急处置报告》，并由安全保障工作小组组长向安全保障领导小组汇报。《后门木马攻击事件应急处置报告》报告内容包括事件处置命令的下达时间、事件处置工作开展时间和结束时间、事件处置人员、事件类型、事件风险分析、事件处置方法、事件处置结果、事件处置建议等方面内容

## 威胁情报事件

### 预案启动条件

威胁情报的定义是在为面临威胁的资产主体(通常为资产所属企业或机构)提供全面的、准确的、与其相关的、并且能够执行和决策的知识和信息。通俗来讲就是对主体有威胁的信息都可以称为威胁情报。

经确定是威胁情报事件后，应当在确认不影响业务系统的前提下，立即启动预案处置工作，无需上报领导小组，但是需要保留相关过程说明记录、处置记录即可。

### 预案执行原则

* 系统恢复原则和业务保障原则

对安全事件原因明确的，应按照系统恢复最快为原则。对于不明原因的安全事件，以对业务保障最有力为原则。

* 及时通报原则

威胁情报安全事件处置过程中要将业务影响情况及时上报领导。

### 预案处置工作

**事件诊断确定**

在攻防演练期间，我们根据威胁情报的来源不同，分为两类：来自外部的威胁情报和来自内部到的威胁情报。

来自内部的威胁情报是指集团或者子公司根据攻击获取到的IP资产。

来自外部的威胁情报是指集团、子公司或者安全厂商从第三方渠道获知IP、源码泄露、集团人员信息泄露、0day、集团信息资产泄露等威胁信息。

**事件现场处理**

威胁情报最终通过各种途径统一汇总到集团总部，由总部攻防演练研判组进行分析研判，确认情报的准确性。

**来自内部的威胁情报**

来自内部的威胁情报目前是指攻击者的IP资产信息。明确威胁情报属性后，我们应采取以下措施：

1. 当集团或者子公司发现攻击者的网络行为或者异常的网络连接，可以将信息汇总传递至总部攻防演练研判组，由研判组进行判别，并统一分发。
2. 封堵IP或者IP段。集团及子公司处置小组收到信息后，IP进行封堵，加入黑名单。一般建议封堵单个IP；但是如果IP较多，可以封堵IP段，之后再进行详细梳理攻击源。

**来自外部的威胁情报**

来自外部的威胁情报范围较为广泛，统指凡是可以对目标系统造成损失或者存在潜在威胁的信息，可以是攻击者IP资产、集团企业源码泄露、集团人员信息大规模泄露、集团网络信息资产大规模泄露、0day等。对于外部的威胁情报信息，可采取以下措施：

1. 当集团、子公司或者第三方获取到相关信息后，立即汇总研判组，进行确认。
2. 对于攻击者IP资产，建议封堵IP或者IP段。集团及子公司处置小组收到信息后，IP进行封堵，加入黑名单。一般建议封堵单个IP；但是如果IP较多，可以封堵IP段，之后再进行详细梳理攻击源。
3. 对于企业集团企业源码泄露、集团人员信息大规模泄露、集团网络信息资产大规模泄露等信息泄露事件，应立即通知领导、责任人进行重大信息泄漏会议，明确处置方式。最后由集团出面和网站等渠道沟通，对相关泄露信息进行封堵。
4. 演练期间有重大漏洞纰漏，应立即由集团和厂商安全人员进行联动，评估对集团的影响，并进行漏洞修复工作。

**事件处置分析**

事件现场处置工作结束后，安全保障工作小组形成《威胁情报事件应急处置报告》，并由安全保障工作小组组长向安全保障领导小组汇报。《威胁情报事件应急处置报告》报告内容包括事件处置命令的下达时间、事件处置工作开展时间和结束时间、事件处置人员、事件类型、事件风险分析、事件处置方法、事件处置结果、事件处置建议等方面内容。