政策与规范

腾讯云安全违规处理

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

腾讯云安全违规处理
客户安全评估工作政策与规范

最近更新时间：2021-08-20 17:42:35

在您购买的腾讯云产品或服务的有效期内，您可对自己部署在腾讯云上的代码、数据、应用、组件等进行安全评估工作。安全评估工作包括但不限于：漏洞扫描、渗透测试、压力测试、漏洞挖掘等（全文同），如果您计划进行安全评估工作，您需同意并遵守以下政策和规范（本协议中也将本政策与规范简称为“本规范”）：

一、您不得对腾讯云基础设施、产品或服务执行任何安全评估工作，包括但不限于服务器、数据库系统、底层应用等。

二、您在进行安全评估工作时，发现任何腾讯云基础设施、产品或服务相关的漏洞，请立即联系腾讯云安全团队（cloud_sec@tencent.com），不得私自公开或向第三方提供相关漏洞的全部或部分信息。

三、您在进行安全评估工作时，不得违反本规范，不得出现评估范围超出您腾讯云账户上所购买和创建的资源范围的情况。

四、您在进行安全评估工作时，如要进行压力测试工作时，需要联系腾讯云安全团队（cloud_sec@tencent.com）进行测试申请。申请时需要提供完整的压力测试方案，申请通过后才可执行压力测试。执行过程中必须严格按照压力测试方案进行。

五、您在进行安全评估工作时，如包含网络钓鱼测试（即，向您的业务使用者发送钓鱼邮件、钓鱼链接、钓鱼文件等行为），您需依法依规开展网络钓鱼测试，且在评估结束后需向业务使用者公开说明网络钓鱼测试行为及测试细节、避免因网络钓鱼行为引起纠纷。如发生用户投诉、纠纷等任何问题，您需自行解决且后果由您自行承担。

六、您在进行安全评估工作时，如涉及对数据、代码等内容进行操作（包括但不限于灾备应急方案评估、对数据或代码进行破坏性操作等），您需要自行做好数据、代码等内容的备份，并自行承担全部后果。

七、您在开展安全评估工作前，应充分了解安全评估工作可能存在的风险，且确保对您安全评估的对象拥有全部合法权利、有权进行安全评估。您需自行承担安全评估工作的全部后果和责任，腾讯云不承担任何由于安全评估工作导致的代码、数据等任何内容丢失，及业务中断、暂停或受影响导致的损失。

八、您在开展安全评估工作前，应充分了解和遵守相关法律法规对相关工作的规定，合法合规开展安全评估工作并遵守本规范的全部要求。如您违反本规范、法律法规、腾讯云服务协议等任何规定，您需自行承担全部责任，并赔偿因此给腾讯云或给其他腾讯云用户等第三方造成的损失。进一步地，您知悉并同意，腾讯云同意您开展压力测试等安全评估工作，并不代表您对压力测试等安全评估行为的免责，如果您在压力测试过程中未按照测试方案执行导致安全事件或是安全评估工作对腾讯云、其他腾讯云用户等第三方造成影响，您仍需承担全部责任，并赔偿因此给腾讯云以及给其他腾讯云用户等第三方造成的全部损失。

违规信息类型说明

最近更新时间：2024-11-27 18:05:52

总则

根据《互联网信息服务管理办法》第十五条，互联网信息服务提供者不得制作、复制、发布、传播含有下列内容的信息：

（一）反对宪法所确定的基本原则的。
（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。
（三）损害国家荣誉和利益的。
（四）煽动民族仇恨、民族歧视，破坏民族团结的。
（五）破坏国家宗教政策，宣扬邪教和封建迷信的。
（六）散布谣言，扰乱社会秩序，破坏社会稳定的。
（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的。
（八）侮辱或者诽谤他人，侵害他人合法权益的。
（九）含有法律、行政法规禁止的其他内容的。

部分违规类型

部分违规类型说明如下：

色情低俗类内容

包括但不限于以下违规内容的信息：

- 散布淫秽、色情内容，包括但不限于招嫖、寻找一夜情、性伴侣等内容。
- 发送以色情为目的的情色文字、情色视频、情色漫画的内容，但不限于上述形式。
- 长期发送色情擦边、性暗示类信息内容，以此来达到吸引用户或进行色情资源交易。
- 直接或隐晦表现性行为、具有挑逗性或者侮辱性内容，或以带有性暗示、性挑逗的语言描述性行为、性过程、性方式的。
- 传播非法性药品、性保健品、性用品和性病治疗营销信息等相关内容的。
- 发布相关部门禁止传播的色情和有伤社会风化、有悖伦理的文字、音视频内容的。

《全国整治互联网低俗之风专项行动方案》中明确的低俗内容：

（1）表现或隐晦表现性行为、令人产生性联想、具有挑逗性或者污辱性的内容。
（2）对人体性部位的直接暴露和描写。
（3）对性行为、性过程、性方式的描述或者带有性暗示、性挑逗的语言。
（4）对性部位描述、暴露，或者只用很小遮盖物的内容。
（5）全身或者隐私部位未着衣物，仅用肢体掩盖隐私部位的内容。
（6）带有侵犯个人隐私性质的走光、偷拍、漏点等内容。
（7）以挑逗性标题吸引点击的。

（8）相关部门禁止传播的色情、低俗小说，音视频内容，包括一些电影的删节片段。
（9）一夜情、换妻、SM 等不正当交友信息。
（10）情色动漫。
（11）宣扬血腥暴力、恶意谩骂、侮辱他人等内容。
（12）非法“性药品”广告和性病治疗广告。
（13）未经他人允许或利用“人肉搜索”恶意传播他人隐私信息。
相关法律法规参考：《中华人民共和国治安管理处罚法》、《中华人民共和国刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》。

危害国家安全、破坏政治与社会稳定类

包括但不限于以下内容：

- 含有分裂国家，破坏国家统一，危害国家安全或利益，破坏政治稳定，煽动颠覆国家政权，推翻社会主义制度，泄露国家秘密的信息。
- 含有歪曲、丑化、亵渎、否定英雄烈士事迹和精神，以侮辱、诽谤或者其他方式侵害英雄烈士的姓名、肖像、名誉、荣誉的信息。
- 含有美化他国侵略史实或宣扬军国主义思想，鼓吹美西价值观的信息。
- 含有宣扬恐怖主义、极端主义或者煽动实施恐怖活动、极端主义活动，煽动民族仇恨、民族歧视，破坏民族团结，散布暴力、凶杀、恐怖或者教唆犯罪的信息。
- 含有散布谣言，扰乱经济秩序和社会秩序，侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的信息。
- 含有法律法规禁止出版发行的书籍、音像制品、视频、文件资料的信息。
- 含有破坏国家宗教政策，非法传教，宣扬邪教、封建迷信的信息。

相关法律法规参考：《中华人民共和国刑法》、《中华人民共和国网络安全法》、《中华人民共和国反分裂国家法》、《中华人民共和国保守国家秘密法》、《互联网信息服务管理办法》、《互联网宗教信息服务管理办法》、《中华人民共和国英雄烈士保护法》、《中华人民共和国反恐怖主义法》、《宗教事务条例》、《互联网宗教信息服务管理办法》。

暴恐血腥类内容

包括但不限于以下违规内容的信息：

- 发送买凶杀人、替人复仇、教唆自杀、收账等具有黑社会性质的信息；雇佣、引诱他人从事恐怖、暴力等活动；拉帮结派，招募成员，对社会秩序构成潜在危害的内容。
- 无资质销售仿真枪、弓箭、管制刀具、气枪等含有杀伤力枪支武器。
- 出现以鼓励非法或鲁莽使用方式等为目的而描述真实武器的内容。
- 散播人或动物被杀、致残以及枪击、刺伤、拷打等受伤情形的真实画面。
- 出现描绘暴力或虐待儿童等内容。
- 出现吸食毒品、自虐自残等令人不安的暴力画面内容。
- 出现事故现场、自杀现场、实验解剖等引起感观不适的血腥内容。

相关法律法规参考：《中华人民共和国治安管理处罚法》、《中华人民共和国刑法》。

赌博类内容

包括但不限于以下违规内容的信息：

- 搭建六合彩，赌球，赌博交易平台。
- 无证从事彩票销售、运营具有博彩性质的棋牌游戏。
- 发布组织聚众赌博、出售赌博器具、传授赌博（千术）技巧、方式、方法等内容、进行博彩活动等。
- 为赌博活动/网站 提供技术服务，包括但不限于提供博彩网站引流、广告宣传、网站代码等。

相关法律法规参考：《中华人民共和国治安管理处罚法》、《中华人民共和国刑法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》。

危害网络安全类内容

包括但不限于以下类型：

- 传播有害程序：通过系统漏洞、应用捆绑下载、网页挂马、电子邮件、即时聊天工具等途径传播病毒、木马等有害程序，对用户正常运行造成损害或中断。
- 网络攻击：通过技术手段对计算机系统、网络或设备进行破坏、干扰、窃取信息或进行其他不当行为的行为。
- 垃圾邮件：向用户发送大量不受欢迎的邮件，例如大量广告或未经授权的推销信息、病毒木马、钓鱼信息等。
- 发布危害网络安全的信息：传播教授各类黑客攻击技术、提供黑客工具下载、售卖黑客工具等。
- 其他违法违规行为：开展违规跨境 VPN、违规提供 DNS 解析服务、开展虚拟币“挖矿”等其他违法违规活动。

相关法律法规参考：《中华人民共和国网络安全法》、《计算机信息网络国际互联网安全保护管理办法》、《中国公用计算机互联网国际联网管理办法》、《国际通信出入口局管理办法》、《中华人民共和国刑法》、《关于办理扰乱无线电通讯管理秩序等刑事案件适用法律若干问题的解释》、《中华人民共和国治安管理处罚法》、《关于依法办理非法生产销售使用“伪基站”设备案件的意见》。

违法经营类

包括但不限于以下违规内容的信息：

- 非法分销、非法集资、非法放贷行为。
- 未取得法定许可证件或牌照、未获得在先的行政许可或未符合监管部门的要求，发布、传播或从事相关经营活动的行为，包括但不限于违规发布药品或医疗器械推广内容的、违规发布证券或期货等投资类有偿咨询内容的、违规发布烟草宣传内容的。
- 以任何形式参与、鼓励、促进或诱导他人排斥正常商业竞争的行为，或为前述行为的传播提供便利的。
- 其它违法经营行为。

相关法律法规参考：《中华人民共和国刑法》、《中华人民共和国刑法》、《电信条例》、《中华人民共和国反不正当竞争法》、《中华人民共和国烟草专卖法》、《中华人民共和国烟草专卖法实施条例》。

违法活动及违禁物品类

包括但不限于以下违规内容的信息：

- 发布或存储国家禁止的违法活动信息（包括发布拐卖妇女、儿童、买卖人体器官、提供赴港代孕中介服务、亲子鉴定服务、胎儿鉴定服务等）。
- 发布或者存储国家禁止出售的化学品的交易信息（包括毒品、剧毒品等）。
- 发布或者存储国家禁止出售的违禁商品/器具类的交易信息（包括军警服装、管制刀具等）。

相关法律法规参考：《中华人民共和国刑法》、《中华人民共和国药品管理法》、《中华人民共和国治安管理处罚法》。

欺诈类内容

包括但不限于以下违规内容的信息：

- 以网站链接提示虚假的中奖信息，以奖金/奖物的中奖信息诱惑用户等。
- 发布钓鱼网站等信息 、伪造正规的网站，利用类似的 URL 的形式，盗取用户的相关信息，诱使用户上当受骗蒙受损失。
- 介绍、讲解、分析、推销、支持被官方认定为网络传销的虚拟货币。
- 以非法占有为目的，用虚构事实或者隐瞒真相的方法，骗取款额较大的公私财物的行为。
- 传销、电信诈骗等信息。
- 虚假金融投资、虚假信用卡待办、网络赌博诈骗等。
- 以虚假交易、交友（杀猪盘）、兼职刷单等手段在网上骗取他人财物。
- 用色情内容低俗内容或赌博内容诱导点击诈骗链接、下载诈骗 App，骗取他人财物。
- 以“民族资产解冻”、“乡村振兴基金”等为由，诱导点击诈骗链接、下载诈骗 App，骗取他人财物。

相关法律法规参考：《中华人民共和国反电信网络诈骗法》、《最高人民法院、最高人民检察院关于办理诈骗刑事案件具体应用法律若干问题的解释》、《中华人民共和国刑法》、《中华人民共和国著作权法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》。

侵权类内容

包括但不限于以下违规内容的信息：

- 外挂、私服等网游类信息；
- 擅自使用他人已经登记注册的企业名称或商标，侵犯他人企业名称专用权及商标专用权；
- 擅自使用他人名称、头像，侵害他人名誉权、肖像权等合法权利。
- 未经授权发布他人身份证号码、照片等个人隐私资料，侵犯他人肖像权、隐私权等合法权益。
- 捏造事实公然丑化他人人格，或用侮辱、诽谤等方式损害他人名誉。
- 未经授权发送企业商业秘密，侵犯企业合法权益。

相关法律法规参考：《中华人民共和国刑法》、《中华人民共和国著作权法》、《全国人民代表大会常务委员会关于维护互联网安全的决定》、《中华人民共和国个人信息保护法》。

云安全违规处罚等级划分说明

最近更新时间：2024-01-05 15:27:52

1. 违规事件分类及处罚说明

用户在使用腾讯云产品时，应遵守国家法律、行政法规、各部门规章等规范性文件，并自行按照相关法律法规，向相关对象提供合法的产品及服务，履行相关义务。对违反相关规定的行为，腾讯云有权进行处罚。

云安全违规事件的分类说明

内容违规

定义：违反国家政策法规及《 腾讯云服务协议 》相关协议、规则，涉及黄、赌、毒、低俗、色情、暴力、侵权等违规内容，如下：

（1）违反宪法确定的基本原则的。
（2）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的。
（3）损害国家荣誉和利益的。
（4）煽动民族仇恨、民族歧视，破坏民族团结的。
（5）破坏国家宗教政策，宣扬邪教和封建迷信的。
（6）散布谣言，扰乱社会秩序，破坏社会稳定的。
（7）散布淫秽、色情、赌博、暴力、恐怖或者教唆犯罪的。
（8）侮辱或者诽谤他人，侵害他人合法权益的。
（9）煽动非法集会、结社、游行、示威、聚众扰乱社会秩序。
（10）以非法民间组织名义活动的。
（11）含有侵害他人名誉权、肖像权、知识产权、商业秘密等合法权利的内容。
（12）涉及他人隐私、个人信息或资料的内容。
（13）发表、传送、传播骚扰信息、广告信息及垃圾信息或含有任何性或性暗示的内容。
（14）含有法律、行政法规禁止的其他内容的。

行为违规

定义：违反国家政策法规及《腾讯云服务协议》相关协议、规则，使用腾讯云产品进行网络恶意行为的，如下：

（1）实施网络拒绝服务攻击、黑客攻击、网络扫描、恶意爬虫等。
（2）实施网络欺诈，网络钓鱼等。
（3）发送垃圾邮件，钓鱼邮件。
（4）传播病毒木马，非法控制其他计算机。
（5）违规提供电信业务等。
（6）因应用遭受大规模 DDoS 攻击影响平台其他开发者正常服务。

2. 云安全违规事件的处理说明

产品分类	对应的违规处罚
CVM/CLB	一般违规行为的相关处罚：阻断 url、阻断网络。
	严重违规行为的相关处罚：阻断网络并禁止解封。
	特别严重违规行为的相关处罚：机器关停、冻结用户相关账户。
EdgeOne/CDN	一般违规行为的相关处罚：阻断 url。
	严重违规行为的相关处罚：加速域名下线。
	特别严重违规行为的相关处罚：服务停用、冻结用户相关账户。
COS	一般违规行为的相关处罚：内容屏蔽。
	严重违规行为的相关处罚：删除文件、冻结 bucket。
	特别严重违规行为的相关处罚：服务停用、冻结用户相关账户。
DNS	一般违规行为的相关处罚：锁定解析记录。
	严重违规行为的相关处罚：域名暂停解析。
	特别严重违规行为的相关处罚：服务停用、冻结用户相关账户。
DNSPOD	一般违规行为的相关处罚：锁定解析记录。
	严重违规行为的相关处罚：域名暂停解析并禁止转移。
	特别严重违规行为的相关处罚：服务停用、冻结用户相关账户。
VOD	一般违规行为的相关处罚：内容屏蔽、删除文件。
	严重违规行为的相关处罚：服务停用。
	特别严重违规行为的相关处罚：冻结用户相关账户。
APIgateway	一般违规行为的相关处罚：单服务停用。
	严重违规行为的相关处罚：单服务停用、不允许新建服务。
	特别严重违规行为的相关处罚：服务停用、冻结用户相关账户。

说明：
一般违规行为、严重违规行为、特别严重行为将根据用户违规次数、违规信息是否造成大量传播，是否情节严重，是否造成严重后果等综合判定。

特别说明

- 如果违规属于特别严重违规，将会对账户进行隔离和清退操作（当月的服务费不退还）。
- 如果因应用遭受大规模 DDoS 攻击影响平台其他开发者正常服务，将有可能对账户进行隔离和清退操作（服务费计算至隔离当日，当日服务费不退还）。
- 如果违规影响面较大，服务将被立即执行隔离操作。
- 如果不是您个人行为导致的违规，那么您的服务器有可能已被恶意入侵，请参见腾讯云提供的 主机安全 产品，寻求解决方案。

安全违规处理帮助指引

最近更新时间：2024-10-24 17:59:52

当您使用腾讯云产品或服务时违反了法律、法规和相关政策，腾讯云将对您的产品、服务或账号进行限制。腾讯云不会主动、或代为清除您存储、发布的违规信息及应用，您可根据本文自行排查处理，确保清理相关内容后提交解封请求。

违规处置记录查询

当腾讯云对您使用的产品、服务或账号进行处置时，会将相关违规信息与处置类型通知您。您可查收账号绑定手机的短信以了解处置通知信息，也可登录邮箱或 站内信 查询处置详细信息（实际接收方式以用户 消息中心 订阅配置为准）。
此外，您可前往 安全管控中心 查询全部处置（或限制）记录，并可进行**申请解封/申诉**等操作。

常见问题

我收到违规告警/违规封禁通知，但不清楚是哪里违规?

有关违规信息类型请查阅 《腾讯云服务协议》 及《违规信息类型说明》。如您未找到相关违规内容，建议您检查下网页源代码是否有植入违规内容，是否有被黑客入侵痕迹。

> **说明：**
> 建议您加强网站的安全防护，降低网站被黑客入侵风险。如您违规次数超过限制，将不再支持解除封禁，详情请参见 《腾讯云信息违规处置等级》 。

违规处置如何申请解封?

确保清理完违规内容后，您可以通过 安全管控中心 申请解封。违规内容排查指引请参考：《违规内容如何排查整改》。

违规处置如何申诉?

若您对违规处置存在异议或不认可违规处置，可通过 违规处置申诉入口 提交诉求，工作人员将在1-3个工作日内给予您反馈。

违规内容如何排查整改?

违规处置排查	1. 检查您的服务是否存在色情、赌博、血腥暴恐等侵害他人合法权益、危害网络安全、国家或社会稳定的违法违规内容； 2. 检查您的腾讯云账号的权限设置和审计日志，确保只有授权人员能够管理和访问您的服务和资源；

	3. 检查您的服务和资源相关页面代码、日志记录、允许其他用户做输入操作的页面等数据中是否存在异常访问或可疑行为的迹象； 4. 排查设备外发流量是否存在异常突增，且非正常业务流量； 5. 排查设备是否运行异常程序，抢占 CPU 等系统资源； 6. 排查设备文件数据是否被异常加密、删除、丢失，且留有勒索信息； 7. 排查设备是否被植入了木马后门，被恶意操控对外攻击； 8. 排查设备是否搭建了网络代理服务（如 frp、HAProxy 等），被恶意利用作为对外攻击跳板； 9. 排查设备是否存在其他可能被入侵利用的高危漏洞； 如您因安全防护措施疏忽，被植入恶意程序，建议备份关键数据后重装系统避免恶意残留；做好系统安全加固，例如设置复杂密码、开启访问限制、定期巡检修复高危漏洞、加强攻击防护措施。
设备被利用从事有害行为	当您的设备被发现用于从事对外攻击等有害网络行为的时候，可能设备已经被恶意利用，我们会暂时限制该设备的访问，以引导您及时排查处理规避风险，您可以按如下步骤处理： 1. 按照指引对被利用的主机进行安全排查，清理进行有害行为的恶意文件，排查指引如下： ○ Linux 主机安全排查指引 ○ Windows 主机安全排查指引 2. 清理完恶意文件后请参考《违规处置如何申请解封》。

被封禁的资源，如何清除违规信息或数据备份?

针对**云服务器 CVM/轻量应用服务器 Lighthouse** 可参考：

1. 当您由于服务封禁导致无法通过标准方式（OrcaTerm）或者远程登录软件登录实例时，您可以使用腾讯云 VNC 登录的方式登录，以便帮助您尽快清除违规内容，具体请参考《无法登录 Windows 实例》或《无法登录 Linux 实例》中“通过 VNC 方式登录”章节。
2. 我们建议您针对重要的业务数据做好备份措施，防止因被动违规而导致的数据安全风险，当实例被封禁后，您可通过创建系统盘快照转为自定义镜像后，共享给新的云服务器/轻量应用服务器排查相关违规并恢复业务数据，数据进一步的备份及恢复请参考《共享自定义镜像》、《数据备份》中的相关章节。

其他请登录腾讯云各产品控制台进行违规内容的清除。

被黑客或病毒侵入，非有意违规如何处理?

被动违规也需要您进行违规内容的清除，可参考《违规内容如何排查整改》有关规则进行排查处理，清理后可参考《违规处置如何申请解封》。

如果对通知内容有异议怎么处理?

若您对通知内容存在异议，可通过 违规处置申诉入口 反馈诉求，工作人员会尽快审核处理。

此类通知后续对我的账号有什么影响?

请您及时处理违法违规内容，并做好账号下使用的腾讯云资源的安全管理。鉴于您名下账号的违规性质及违规程度，腾讯云根据《中华人民共和国网络安全法》、《电信业务经营许可管理办法》及《腾讯云服务协议》等相关规定，有权限制、暂停、终止向您提供部分或全部产品和服务。

如何修改通知接收人?

处置通知以站内信、邮件、短信等方式触达，如需修改联系方式可前往 订阅管理页面 中修改安全事件通知接收人。具体操作详情请参见 消息订阅管理 。

被动违规排查指引

最近更新时间：2025-06-05 10:17:42

场景一：告警定位到具体资源（图片等内容违规）

明确告知某资源（如 `/document/illegal_image.jpg` ）为违规内容，若非主动上传，则通常由第三方恶意上传导致。

排查方式

1. 检查上传渠道安全性
   a. 审查网站是否存在文件上传和存储服务。
   b. 检查上传功能模块是否校验文件类型、文件内容等。
2. 检查数据库关联
   a. 检查数据库是否存在无关账号。
   b. 检查数据库权限配置是否遵循最小必要原则。
3. 恶意文件排查
   a. 参考 恶意文件处理 ，登录 主机安全控制台 ，选择**入侵检测 > 文件查杀**，使用实例 ID 进行查询、隔离或清除文件，增加防护策略。

解决方案

- 立即删除违规文件，并清理相关缓存，避免违规内容继续传播。
- 对上传文件进行严格的类型校验、大小限制，并人工审核。
- 将开源 CMS、数据库等升级为最新版本，采用预编译等必要防护措施。
- Linux 安全加固 、Windows 安全加固 。

场景二：告警定位到正常页面（URL 存在恶意跳转）

访问违规 URL 时自动跳转至恶意网站（如钓鱼网站、恶意软件下载页），若非主动违规，则通常由黑客入侵导致。此类跳转通常具有隐蔽性，需要在特定时间和环境下访问触发。

排查方式

1. JS 跳转排查
   a. 检查网站页面的 JavaScript 代码，查看是否存在异常的 `window.location.href` 跳转语句，特别是未经过授权的跳转代码，定位代码中恶意插入的跳转逻辑。
2. 配置文件检查
   a. 检查网站的配置文件（如 .htaccess、web.config、nginx.conf），确认是否被篡改，查看是否存在恶意的重定向规则。
   b. 检查应用程序的配置参数，如跳转链接地址是否被修改为恶意网址。

3. DNS 恶意解析排查

a. 使用 `nslookup` 或 `dig` 命令，检查域名解析结果是否正确，对比不同 DNS 服务器（如8.8.8.8、114.114.114.114）的解析结果，确认是否存在 DNS 劫持（如解析到异常 IP 地址）。

b. 检查本地 hosts 文件，查看是否被写入恶意域名解析记录。

4. 恶意文件排查

a. 参考 恶意文件处理，登录 主机安全控制台，选择**入侵检测 >文件查杀**，使用实例 ID 进行查询、隔离或清除文件，增加防护策略。

解决方案

- 恢复被篡改的内容，加强配置文件的访问权限控制，仅允许授权用户修改。
- 联系域名服务商或网络管理员，排查 DNS 劫持问题，修复 DNS 解析记录。
- 将开源 CMS、数据库等升级为最新版本，采用预编译等必要防护措施。
- Linux 安全加固、Windows 安全加固。

相关法律法规

最近更新时间：2020-09-02 16:43:03

- 中华人民共和国网络安全法
- 互联网域名管理办法
- 网络信息内容生态治理规定
- 移动互联网应用程序信息服务管理规定
- 《信息产业部关于做好互联网网站实名管理工作的通告》信部电〔2007〕338号
- 计算机信息网络国际联网安全保护管理办法
- 中华人民共和国电信条例
- 全国人民代表大会常务委员会关于加强网络信息保护的决定
- 互联网信息服务管理办法
- 互联网电子公告服务管理规定
- 互联网危险物品信息发布管理规定
- 互联网信息搜索服务管理规定
- 互联网视听节目服务管理规定
- 互联网用户账号名称管理规定
- 互联网跟帖评论服务管理规定
- 互联网论坛社区服务管理规定
- 互联网直播服务管理规定
- 网络出版服务管理规定
- 最高人民法院、最高人民检察院、公安部关于办理网络赌博犯罪案件适用法律若干问题的意见
- 最高人民法院最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释
- 最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二）
- 最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定

安全课堂

最近更新时间：2020-09-02 16:43:51

重要的信息化系统需要操作留痕、数据加密

《网络安全法》第二十一条规定：
国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。
（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施。
（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。
（四）采取数据分类、重要数据备份和加密等措施。
（五）法律、行政法规规定的其他义务。
解读：
对于内部安全管理应从两方面实施，一方面制定内部安全管理制度，所有操作人员必须按制度严格规范操作；另一方面采用运维审计系统（如：堡垒机、数据库审计等）进行日常工作，对操作流程全程记录并保存相关日志便于事后取证。 对重要数据（如：企业和个人邮箱等）进行加密确保数据的可靠性（如：邮箱加密系统等）。
法律责任补充，第六章第五十九条，网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

网站被入侵、劫持或将导致网站运营者被罚款

《网络安全法》第二十一条规定：
网络运营者应当履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。
（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施。
（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。
（四）采取数据分类、重要数据备份和加密等措施。
解读：
主机，网站日常安全维护必不可少，不要因为平常运营没出现问题就掉以轻心不去管理，一旦主机，网站被入侵，带来的危险性就非常大，轻则数据丢失，重则负法律责任。
第五十九条规定 网络运营者不履行本法第二十一条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

系统不做等保将被处罚

《网络安全法》第二十一条规定：
网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
解读：
要求网络运营者按网络安全等级保护制度规定，制定内部安全管理制度和操作规程，确定负责人，建立全面安全体系，采用防范和记录计算机病毒和网络攻击、网络侵入等多种危害网络安全行为的技术措施； 法律责任补充：第六章第五十九条：拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款；对直接负责的主管人员处五千元以上五万元以下罚款。

用户信息泄露，可能导致停业

《网络安全法》第四十二条规定：
（一）网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。
（二）网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
解读：
网络运营者对于个人数据在使用、交换、交易过程中都要合法。确保个人数据在使用共享时不泄密，又能被充分利用，网络运营者应该对于个人信息有专门的安保措施，需要持续加强数据库的安全防护。监控来自内外部的数据不安全成为关键。
法律责任补充：第六章第六十四条，对于侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。