|  |  |  |  |
| --- | --- | --- | --- |
| XX事业部网络安全事件  应急响应报告 | | | |
| ■ 文档编号 | 04 | ■ 密级 | 商业机密 |
| ■ 版本编号 | v1.0 | ■ 日期 | 2017-XX-XX |

|  |  |  |  |
| --- | --- | --- | --- |
| ■ 变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
| 2017-XX-XX | V1.0 | 创建文档 | XXX |

1. 业务信息

|  |  |  |  |
| --- | --- | --- | --- |
| **业务线名称** | | | |
|  | | | |
| **业务线联系人** | | | |
| **姓名** |  | **邮箱** |  |
| **电话** |  | **微信** |  |

1. 应急人员

|  |  |  |  |
| --- | --- | --- | --- |
| **应急人员信息** | | | |
| **姓名** |  | **所属部门** | 运维安全部 |

1. 事件概述

|  |  |
| --- | --- |
| **事件现象** |  |
| **处理时间** |  |
| **完成时间** |  |
| **关键字词** |  |
| **服务器IP** | 如公网、私网地址 |
| **机房的位置** | 如大兴机房、aliyun华北一区机房 |
| **绑定的域名** | 如a.com |
| **服务的功能** | 如后台存储服务 |
| **服务的框架** | 如struts，weblogic，wordpress，discuz，django |
| **服务的组件** | 如Redis、Mongodb、Mysql、Weblogic |
| **Web的目录** | 如/var/www/html/ |
| **Web的日志** | 如/var/log/html/ |
| **防火墙策略** | 如Iptables-save的输出 |
| **周边的环境** | 如同一网段内xxx.xxx.xxx.xxx在xxxx年xx月xx日因为xx原因被入侵 |

1. 处理过程

|  |
| --- |
| **处理过程描述** |
|  |
| **处理过程记录** |
|  |

1. 结论建议

|  |
| --- |
| **结论建议** |
| **结论：** |
| **建议：** |

1. 附件列表