**提前检查**

1. 服务器和网站漏洞检测，对Web漏洞、弱口令、潜在的恶意行为、违法信息等进行定期扫描。
2. 代码的定期检查，安全检查，漏洞检查。
3. 服务器安全加固，安全基线设置，安全基线检查。
4. 数据库执行的命令，添加字段、加索引等，必须是经过测试检查的命令，才能在正式环境运行

**数据备份**

1. 服务器数据备份，包括网站程序文件备份，数据库文件备份、配置文件备份，如有资源最好每小时备份和异地备份。
2. 建立五重备份机制：常规备份、自动同步、快照。
3. 定期检查备份文件是否可用，避免出故障后，备份数据不可用。
4. 重要数据多重加密算法加密处理。
5. 程序文件版本控制，测试，发布，故障回滚

**安全监控**

1. zabbix或cacti监控服务器常规状态CPU负载、内存、磁盘、流量等状态，可以显示历史曲线，方便排查问题。
2. 监控服务器SSH登录记录、iptables状态、进程状态，有异常记录告警。
3. 监控网站WEB日志（包括nginx日志php日志等），可以采用EKL来收集管理，有异常日志告警。
4. 运维人员都要接收告警邮件和短信，至少所负责的业务告警邮件和短信必须接收，运维经理接收重要业务告警邮件和短信。
5. 除服务器内部监控外，最好使用第三方监控，从外部监控业务是否正常（监控URL、端口等）

**故障避免预防**

1. 网站WEB增加WAF，避免XSS跨站脚本、SQL注入、网页挂马等漏洞威胁。
2. 程序代码连接数据库、memcache、redis等，可以使用域名（域名HOSTS指定IP），当出问题，有备用的服务器，就可以通过修改DNS或者HOSTS，恢复服务。
3. 建立应急预案机制，定期演练事故场景，估算修复时间。
4. 部署蜜罐系统，防范企业和服务器内网APT攻击。
5. 建立双活集群，包括业务服务的高可用，避免业务服务单点。
6. 服务器集群采用跳板机或堡垒机登录，避免服务器集群每台服务器可以远程连接管理。
7. 操作重要业务升级、迁移、扩容……之前，列一下操作步骤，越详细越好，实际操作按步骤操作，操作完做好记录。

**事中操作**

1. 网站WEB增加WAF，发现XSS、SQL注入、网页挂马等攻击，会自动拦截，并记录日志。
2. 检查服务器数据备份是否可用。
3. 在处理需求和故障时，执行风险命令（比如rm、restart、reboot等）需再三确认，执行命令前，检查所在服务器，所在服务器路径，再执行！
4. 不要疲劳驾驶，喝酒不上机，上机不喝酒，尤其别动数据库，避免在不清醒的状态下，在服务器上执行了错误命令，导致数据丢失或业务故障。
5. 在处理事故时，一定要考虑处理措施是否会引发连锁故障，重要操作三思而行

**事后检查分析**

1. 实现网络安全可视化管理，可以看到每天有那些异常IP和异常URL请求，服务器集群开放端口列表等。
2. 能对全网进行安全策略集中管理。
3. 统一日志收集和分析。
4. 备份及篡改恢复功能，程序文件、图片、数据文件、配置文件的备份，故障回滚机制。
5. 对攻击日志进行深度分析，展现攻击路径、攻击源，协助管理员溯源。
6. 践行DevOps的无指责文化，尤其是在做事故分析时。事故分析重在定位原因，制定改进措施。