驿来特平台安全

一、 平台硬件

目前，微信公众号管理功能模块上线了运维监控功能，可以实现域名、账户余额、数据库实例或 MongoDb 实例、Redis 实例的 CPU 磁盘情况等情况的监控，同时，也可以提示到期时间等功能，对于未尽的监控事宜，可以考虑要求增加功能即可完成监控。经观察，上线一个月多的时间内，Mysql 数据库的磁盘由原来的 40GB，增加到 46GB，增长过快，按这个速度，一年后就是将近 100G，而 100GB 的 Mysql 数据库在性能上是无法正常工作的，亟需解决主数据库磁盘增长过快的问题，不能等到问题发生时才关注。解决思路如下：

1、 哪个表增长过快？
2、 是否可以考虑迁移到历史库？

这个工作虽然无法带来业务上的增长，但可以保证业务系统健康的运行，也是非常重要的工作，需要未雨绸缪。

二、 防护措施

1.网络安全层面：云防火墙，通过 ACL 访问控制策略，对于需要接入的平台允许放行，对于没有访问需求的 IP 进行阻断。实现精细的访问控制策略。通过云防火墙的内置入侵防御模块，对于网络攻击、病毒传播都有较好的防护效果。

2.应用层面：Web 应用防火墙，通过 CNAME 的接入方式将域名接入 WAF，可以隐藏您的网站源 IP，对于所有请求进行分析和识别，将具备攻击行为的请求进行拦截。利用区域封禁功能拦截境外不需要访问的 IP；扫描防护攻击将一些恶意扫描拦截；BOT 管理可以拦截爬虫、IDC 等机器行为。

3.主机层面：云安全中心，使用云安全中心对主机进行防护、可以针对病毒、漏洞、入侵攻击、恶意行为、暴力破解等行为进行识别和防御。还支持主机防勒索和数据库防勒索功能。

三、 维护制度

1、 数据库只进行了备份，未按等保要求进行定期的恢复实验不能保证备份的东西我们就一定能恢复，需要制订制度由专人定期（比如每月 1 次）进行全量恢复实验，增量的采用 RedoLog 日志进行恢复实验，保证随时可以更新到出故障的最后一刻。实验完成后，需要实验人员签字留痕。
2、 购买阿里云提供的漏洞扫描服务对软件系统进行定期扫描一来是由于系统在不断的增加代码，带来更多风险，二来是 Java 或系统的缺陷会随时间的增长而更多的暴露出来，

漏洞库也在不断的更新，建议每 3 个月增加一次扫描工作。[1]

3、 进行空难性故障恢复演练，梳理出异常情况下快速恢复服务的方法和路径。