系统安全方案

随着某某项目的不断深入，各部分系统都涉及到业务数据，客户资料等不可泄漏的数据，软件系统的安全，服务器的安全，微信公众平台的帐号安全，服务器的负载问题都变得尤为重要。对此，给出安全方案。

□□ **微信公众平台安全方案**

目前某某的微信公众帐号已经开通及认证，并且实现自助报价，网店、定损点查询等几项功能。微信公众平台作为企业公众形象的一个窗口，并且具有营销、服务客户、宣传等功能，未来也会有越来越大的客户量，各种因素都决定了该平台必须有完善严格的安全方案。

首先是账户的安全，微信平台的登录流程很简单，只需要用户名和密码，这就决定了一旦用户名和密码泄漏，整个平台就不会失去控制，给用户和公司都造成很坏的影响。对于账户和密码的安全维护，必须是人为的控制，做好维护。

平台的维护主要依靠内部力量同时依靠外部力量相结合的办法，可以设置管理员、微信平台专职发送人员做好日常维护工作，负责微信平台的稳定、可靠、安全运行。该平台由部门委派专人管理。平台使用采用批示制度，文件内容至少应包括：操作人、操作原由、发送对象或群体、发送内容、操作人签字、管理人签字。对帐号和密码做严格保密处理，并且只能在规定机器上登录。

微信平台推送消息有两个唯一参数，在后台程序中被写死，这两个参数一旦泄漏，即使不使用密码登录，也可以给用户推送消息，这也造成参数的不可泄漏性，后台程序的不可泄漏性，这个安全隐患主要通过对服务器的防护实现，将在后面服务器安全方案提到。

有安全防护措施的前提下，依然要做最坏的准备，一旦帐号密码、参数程序等泄漏，要有应对措施。重要的是后台要实时有维护人员，一旦发现异常，立即更改密码，尽快查找漏洞。

二、服务器的安全方案

目前某某项目涉及到多项系统，这些软件系统的安全最重要的部分都在于所部属服务器安全，所以要尽最大可能保证服务器安全。

在服务器硬件方面，可以通过高可用集群、双机热备策略，应对服务器瘫痪，被黑，负载过重给系统带来的影响。

高可用性集群，英文原文为High Availability Cluster, 简称HA Cluster，是指以减少服务中断（宕机）时间为目的的服务器集群技术。简单的说，集群（cluster）就是一组计算机，它们作为一个整体向用户提供一组网络资源。这些单个的计算机系统就是集群的节点（node）。一个理想的集群是，用户从来不会意识到集群系统底层的节点，在他/她们看来，集群是一个系统，而非多个计算机系统。并且集群系统的管理员可以随意增加和删改集群系统的节点。

高可用集群不是用来保护业务数据的，保护的是用户的业务程序对外不间断提供服务，把因软件/硬件/人为造成的故障对业务的影响降低到最小程度。

所谓双机热备，其实可以认为是集群的最小组成单位，就是将中心服务器安装成互为备份的两台服务器，并且在同一时间内只有一台服务器运行。当其中运行着的一台服务器出现故障无法启动时，另一台备份服务器会迅速的自动启动并运行（一般为

为数分钟左右），从而保证整个网络系统的正常运行！双机热备的工作机制实际上是为整个网络系统的中心服务器提供了一种故障自动恢复能力。

为提高服务器的使用效率，也不影响服务器的性能，在工作方式选择上，有如下的选择：

1、主/主 (Active/active)

这是最常用的集群模型，它提供了高可用性，并且在只有一个节点在线时提供可以接受的性能，该模型允许最大程度的利用硬件资源。每个节点都通过网络对客户机

提供资源，每个节点的容量被定义好，使得性能达到最优，并且每个节点都可以在故障转移时临时接管另一个节点的工作。所有的服务在故障转移后仍保持可用，但 是性能通常都会下降。

2、主/从(Active/passive)

为了提供最大的可用性，以及对性能最小的影响，Active/passive模型需要一个在正常工作时处于备用状态，主节点处理客户机的请求，而备用节点处于空闲状态，当主节点出现故障时，备用节点会接管主节点的工作，继续为客户机提供服务，并且不会有任何性能上影响。

3、混合型(Hybrid)

混合是上面两种模型的结合，只针对关键应用进行故障转移，这样可以对这些应用实现可用性的同时让非关键的应用在正常运作时也可以在服务器上运行。当出现故

障时，出现故障的服务器上的不太关键的应用就不可用了，但是那些关键应用会转移到另一个可用的节点上，从而达到性能和容错两方面的平衡。

考虑到系统的负载，以及成本原因，使用软件热备方案就可以实现安全需求了，工作方式选择主/主即可。

对服务器安全而言，安装防火墙非常必要。防火墙对于非法访问具有很好的预防作用，硬件防火墙和软件防火墙我认为都是必备的。

在做好硬件防护的同时，软件层面也很重要。最小的权限+最少的服务=最大的安全。在软件维护方面，有几个策略：

1、从基本做起，及时安装系统补丁

不论是Windows还是Linux,任何操作系统都有漏洞，及时的打上补丁避免漏洞被蓄意攻击利用，是服务器安全最重要的保证之一。

2、安装和设置防火墙

现在有许多基于硬件或软件的防火墙，很多安全厂商也都推出了相关的产品。对服务器安全而言，安装防火墙非常必要。防火墙对于非法访问具有很好的预防作用，但是安装了防火墙并不等于服务器安全了。在安装防火墙之后，你需要根据自身的网络环境，对防火墙进行适当的配置以达到最好的防护效果。

3、安装网络杀毒软件

现在网络上的病毒非常猖獗，这就需要在网络服务器上安装网络版的杀毒软件来控制病毒传播，同时，在网络杀毒软件的使用中，必须要定期或及时升级杀毒软件，并且每天自动更新病毒库。

4、关闭不需要的服务和端口

服务器操作系统在安装时，会启动一些不需要的服务，这样会占用系统的资源，而且也会增加系统的安全隐患。对于一段时间内完全不会用到的服务器，可

以完全关闭;对于期间要使用的服务器，也应该关闭不需要的服务，如Telnet等。另外，还要关掉没有必要开的TCP端口。

5、定期对服务器进行备份

为防止不能预料的系统故障或用户不小心的非法操作，必须对系统进行安全备份。除了对全系统进行每月一次的备份外，还应对修改过的数据进行每周一次的备份。同时，应该将修改过的重要系统文件存放在不同服务器上，以便出现系统崩溃时(通常是硬盘出错)，可以及时地将系统恢复到正常状态。

6、账号和密码保护

账号和密码保护可以说是服务器系统的第一道防线，目前网上大部分对服务器系统的攻击都是从截获或猜测密码开始。一旦黑客进入了系统，那么前面的防卫措施几乎就失去了作用，所以对服务器系统管理员的账号和密码进行管理是保证系统安全非常重要的措施。

7、监测系统日志

通过运行系统日志程序，系统会记录下所有用户使用系统的情形，包括最近登录时间、使用的账号、进行的活动等。日志程序会定期生成报表，通过对报表进行分析，你可以知道是否有异常现象。

当然再稳妥完善的安全措施也有可能有疏漏之时，应对措施是必备的。首先针对服务器，关键是软件系统的监控很重要，目前可以使用监控软件，针对这块的解决方法有:URL监控:对企业关键的WEB网站，通过内容匹配、页面文件大小检查、页面文件修改时间检查的技术手段，确保网站受到黑客威胁时迅速发出报警通知。对于服务器的监控主要针对:硬件状态监控，性能监控，应用服务监控，

针对服务器的事件日志的监控，出现异常，会有图形界面、电子邮件、短信等方式的报警。

一旦系统被黑，需要立即做出处理，包括：

1、立即停止系统服务，避免用户继续受影响，防止继续影响其他站点。

□□

2、如果同一主机提供商同期内有多个站点被黑，您可以联系主机提供商，敦促对方做出应对。

□□

3、清理已发现的异常，排查出可能的被黑时间，和服务器上的文件修改时间相比对，处理掉黑客上传、修改过的文件;检查服务器中的用户管理设置，确认是否存在异常的变化;更改服务器的用户访问密码。

□□

注：可以从访问日志中，确定可能的被黑时间。不过黑客可能也修改服务器的访问日志。

□□4、做好安全工作，排查网站存在的漏洞，防止再次被黑。

三、后台程序的安全方案

目前项目多系统后台程序偏多，如果做不好程序的安全维护，一旦程序丢失、被黑，会严重影响整个系统的正常运行。对于这方面主要由开发人员和后期维护人员的完成。首先要做好数据备份，保证出现问题时迅速恢复。其次程序的日志部分要完善，做好程序文件的巡检工作，做好程序文件的修改增删记录。