网站安全，我们需要注意的

产品名称	网站安全，我们需要注意的
公司名称	广州数据猫网络科技有限公司
价格	.00/个
规格参数	机房:佛山/江苏等 租赁周期:年/月 套餐:200G/300G等
公司地址	广州市天河区灵英东路3号
联系电话	17701938714 15625004753

产品详情

防御DDOS流量攻击。找梁经理199-2742-9680V电同号，CC防御，DDOS防御CC攻击，专业防御DDOS攻击，DDOS防御流量攻击，DDOS防CC流量攻击，DDOS防御，防御DDOS攻击，防御CC攻击。

网站安全是指出于防止网站受到外来电脑入侵者对其网站进行挂马，篡改网页等行为而做出一系列的防御工作。启动一个新网站是一个令人兴奋的项目，充满了许多重要的步骤和决定。但是，作为网站的所有者，您不仅要处理被黑客入侵的后果，还要对其页面上的内容以及人们用来与之交互的机制负责。如果您计划存储用户信息（例如密码或电话号码），则必须妥善保护这些数据，否则根据某些法律，您可能会因数据泄露事件而受到罚款。

如果网站被黑客攻击了之后，要如何处理呢？

1、发现服务器被入侵，应立即关闭所有网站服务，暂停至少3小时。

2、下载服务器日志，并且对服务器进行全盘杀毒扫描。

3、Windows系统打上zui新的补丁，然后就是mysql或者sql数据库补丁，还有php以及IIS，serv-u就更不用说了，经常出漏洞的东西，还有就是有些IDC们使用的虚拟主机管理软件。

4、完成以上步骤后，您需要把管理员账户密码，以及数据库管理密码，特别是sql的sa密码，还有mysql的root密码，要知道，这些账户都是具有特殊权限的，黑客可以通过他们得到系统权限!

5、关闭删除所有可疑的系统帐号，尤其是那些具有高权限的系统账户!重新为所有网站目录配置权

限，关闭可执行的目录权限，对图片和非脚本目录做无权限处理。

企业网站常见的安全问题：

1.数据泄露

网站是企业对外开放的门户，因此会成为黑客利用获取数据的主要手段，黑客窃取企业重要数据，用来攻击企业网站或勒索企业，给企业带来经济损失。.

2.网页篡改

企业网页被篡改，不仅会降低网站浏览用户的体验感，还会导致网站面临运营风险。所以企业一定要重点关注，保证网页不被篡改；

3.服务器系统漏洞

利用服务器系统漏洞是网站遭受攻击的常见方式，网站基于计算机网络，而计算机运行少不了操作系统。操作系统漏洞会直接影响网站安全，一个小小的系统漏洞可致系统瘫痪，比如缓冲区溢出漏洞、IIS漏洞、第三方软件漏洞等。

4.DDoS攻击

浏览网站是需要启动TCP连接的，服务器一旦接收到第1个数据包，就会返回一个响应。然后，设置zui终的ACK数据包并关闭连接。当您使用计算机访问网站时，此过程在后台进行。而DDoS攻击利用TCP协议，通过大量虚假IP向服务器发送数据包，然后在目标服务器以开放连接响应时不响应。攻击者将大量流量重定向到网站，导致无数连接超时，zui终导致服务器性能崩溃。

那么网站安全解决方案有哪些呢？

1、安全巡检

定期对网站进行安全检测，全面排查安全风险点并提供加固。

2、漏洞监测

采取系统安全软件自动监测与人工监测相结合的方法，人工定期或不定期的对服务器和程序做漏洞扫描和处理，系统安装的安全软件实时对zui新爆发的高危漏洞及时预警监测，轻松防范攻击。

3、系统加固

严格设置网站和服务器文件上传目录权限，开启驱动级文件防篡改，保护指定目录下的文件不被修改，严格管理写入权限；IP黑白名单自动拦截恶意IP访问；SQL防注入，防止黑客通过Web服务器或Web应用程序的漏洞入侵服务器；智能检测并防御CC攻击，保证网站正常服务能力；通过增强远程登录认证方式来防止非法用户入侵服务器。

4、数据备份

云服务器用户开通自动快照，可以选择每天、每小时或根据客户要求对服务器数据进行自动快照，避免因黑客攻击或各种原因造成的数据丢失，虚拟空间用户根据和我单位的网站维护约定，我单位

有自动快照设置和专人进行人工备份，防止您的重要数据丢失。

5、程序升级

对后台程序、数据库、防火墙等及时升级版本。

企业网站的安全对于企业的正常运行非常重要，企业一定要做好日常防护并接入高防服务作为辅助，来对抗网络安全问题，避免其给企业带来的不必要损失。

本文部分摘自网络，如有不便，请及时联系删除