一键搞定“等保”和“密保”合规保障措施

“等保”就是网络安全等级保护的简称，等级保护 2.0 标准体系是根据《网络安全法》第二十一条“国家实行网络安全等级保护制度”和第三十一条“国家对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”的要求重新调整和修订等级保护 1.0 标准体系，配合《网络安全法》的实施和落地，指导用户按照网络安全等级保护制度的新要求，履行网络安全保护义务。而“等保测评”则是测评机构依据国家信息安全等级保护制度规定，对非涉及国家秘密信息系统安全等级保护状况进行检测评估的活动，是各种信息系统安全等级保护的合规要求。

“密保”是密码保护的简称，根据《密码法》第二条“密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务”和第二十七条“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护”的要求而实现的对信息系统的安全保护。而对应的“密评”则是商用密码应用安全性评估的简称，是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估，也是各种信息系统安全的合规要求。《密码法》第二十七条同时要求关键信息基础设施运营者需自行或者委托商用密码检测机构开展商用密码应用安全性评估。商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。

总结一句话就是：关键信息基础设施必须同时满足《网络安全法》和《密码法》的合规要求，政府网站和一网通办系统就属于关键信息基础设施。但是，根据国家互联网应急中心 4 月 26 日发布的第 17 期《网络安全信息与动态周报》数据，一周内有 738 个网站被植入后门，其中有 12 个政府网站。一周内有 3611 个网站被篡改，其中有 17 个政府网站。而 2020 年我国境内 53,171 个网站被植入后门，其中政府网站有 256 个。从这些数据可以看出，还有不少网站

仍然处于没有防护的状态中，特别是还有政府网站，这是已经严重违法了！怎么办？

零信网站安全云服务可以帮助这些网站包括政府网站一键实现“等保”合规要求，一键实现“密保”合规要求。用户只需设置一次 CNAME 域名解析，完成域名控制权验证，就可以自动完成网站 SSL 证书的申请，一键满足密码合规要求。再设置一次 CNAME 域名解析，就可以自动启动阿里云 WAF 服务，并自动把绑定用户网站域名的 SSL 证书配置到阿里云 WAF 中同时实现网站 https 加密和 WAF 防护。只需两次一键设置就完美地同时实现了“等保”和“密保”的关键部分要求。

阿里云 WAF 能满足用户在“入侵防范”、“恶意代码防范”、“数据完整性(防篡改)”等三个方面的等保合规要求的，并且是一键实现。而零信云 SSL 则不仅能满足用户在“通信传输”、“数据完整性”、“数据保密性”等三个方面的等保合规要求，同时还能满足用户在“网络与通信安全”-采用密码技术保证通信过程中数据的完整性、机密性和实体身份的真实性、“应用和数据安全”-采用密码技术保障信息系统应用的重要数据在传输、存储过程中的机密性和完整性等两个方面的密保合规要求，也是一键实现。

零信网站安全云服务是一个把满足等保合规要求的阿里云 WAF 服务和满足密保合规要求的 https 加密服务打包成一个全自动实现 WAF 防护和 https 加密的创新服务，不仅大大降低了网站安全合规成本，而且也是最重要的，保护了网站重要的数据安全，保障了网站业主的正常

业务顺利运行。合规是一方面，保护自己的重要业务数据更重要！零信网站安全云服务，让天下所有网站尽享天天安全无忧！

王高华

2022 年 6 月 1 日于深圳

请关注公司公众号，实时推送公司 CEO 精彩博文。